

INFORMATION PROCESSOR COLLECTING AND MANAGING LOG DATA

Publication number: JP10293704 (A)

Publication date: 1998-11-04

Inventor(s): FUJINO SHUJI; MORIKAWA TOSHIYOSHI; URANO AKIHIRO;
NAKANAO HIDENORI; MORITA SHINJI; YAMADA MITSUGI;
NIMURA YOSHITAKA *

Applicant(s): HITACHI LTD *

Classification:

International: G06F11/00; G06F11/34; (IPC1-7): G06F11/34

European: G06F11/00; H04L12/24A4; H04L12/24D

Application number: JP19970101210 19970418

Priority number(s): JP19970101210 19970418

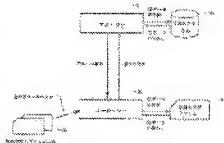
Also published as:

JP3778652 (B2)

US6173416 (B1)

Abstract of JP 10293704 (A)

PROBLEM TO BE SOLVED: To manage log data based on a common data format and also to manage log data based on the time of a manager in a system in which a manager collects log data from plural agents through a network. **SOLUTION:** A manager 10 distributes various rules to an agent 20. The agent 20 inputs log data from a monitored object log file group 30 according to the rules, normalizes it, adds the correction time of a log output time and stores it in a normalization log file 40. The agent 20 fetches normalization log data from the file 40 and transfers it to the manager 10 according to a request from the manager 10. The manager 10 stores collected normalization log data in a normalization log database 50 in order of the correction time.



Data supplied from the **espacenet** database — Worldwide

特開平10-293704

(43)公開日 平成10年(1998)11月4日

(51)Int.Cl.⁶

G 0 6 F 11/34

識別記号

F I

G 0 6 F 11/34

B

審査請求 未請求 請求項の数5 O L (全 24 頁)

(21)出願番号

特願平9-101210

(22)出願日

平成9年(1997)4月18日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72)発明者 藤野 修司

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内

(72)発明者 森川 孝義

東京都千代田区大手町二丁目6番2号 株式会社日立情報ネットワーク内

(72)発明者 清野 明裕

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74)代理人 弁理士 高橋 明夫

最終頁に続く

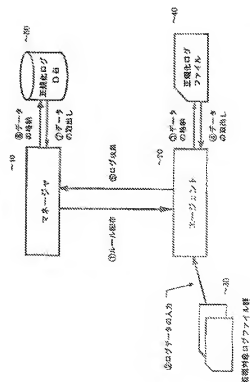
(54)【発明の名称】 ログデータの収集と管理をする情報処理装置

(57)【要約】

【課題】 マネージャがネットワークを介して複数のエージェントからログデータを収集するシステムにおいて、共通的なデータ形式に基づいてログデータを管理する。またマネージャの時刻に基づいたログデータを管理する。

【解決手段】 マネージャ10は、各種ルールをエージェント20に配布する。エージェント20は、このルールに従って監視対象ログファイル群30からログデータを入力し、正規化し、ログ出力時刻の補正時刻を付加して正規化ログファイル40に格納する。マネージャ10からの要求に従ってエージェント20は、正規化ログファイル40から正規化ログデータを取り出してマネージャ10へ転送する。マネージャ10は、収集した正規化ログデータを補正時刻の順に正規化ログデータベース50に格納する。

図2



【特許請求の範囲】

【請求項1】監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成して蓄積する手段と、蓄積された正規化ログデータをネットワークを介してマネージャの機能を実行する情報処理装置へ送信する手段とを有するコンピュータプログラムであることを特徴とするログデータの収集をする情報処理装置。

【請求項2】コンピュータ読み取り可能な記憶媒体上に実体化され、ログデータを収集するエージェント機能を有するコンピュータプログラムであって、該プログラムは以下のステップを含む：

(a) 監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成し、(b) 蓄積された正規化ログデータをネットワークを介してマネージャの機能を実行するコンピュータへ送信する。

【請求項3】ネットワークを介してエージェントの機能を実行する情報処理装置からあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信する手段と、該正規化ログデータを補正時刻の順にデータベースに蓄積する手段とをマネージャの処理手段として有することを特徴とするログデータの収集と管理をする情報処理装置。

【請求項4】該補正時刻とマネージャの現在時刻との差分の時間が所定の保存期間を超過している正規化ログデータを該データベースから削除する手段をさらに設けることを特徴とする請求項3記載のログデータの収集と管理をする情報処理装置。

【請求項5】コンピュータ読み取り可能な記憶媒体上に実体化され、ログデータの収集と管理をするマネージャ機能を有するコンピュータプログラムであって、該プログラムは以下のステップを含む：

(a) ネットワークを介してエージェントの機能を実行するコンピュータからあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信し、(b) 該正規化ログデータを補正時刻の順にデータベースに蓄積する。

【発明の詳細な説明】

【0001】
【発明の属する技術分野】本発明は、マネージャがネットワークを介してエージェントからログデータを収集するシステムに係わり、特にマネージャがシステム内に存在するログデータを共通的なログデータ形式に基づいて管理するログデータの収集と管理の方法に関する。

【0002】

【従来の技術】情報処理装置で実行されるオペレーティングシステム（OS）やアプリケーションプログラムは、各種のログ情報を出力する。出力されたログ情報は、収集するいくつかの方法が知られている。例えば特開平5-250229号公報は、複数のコンピュータからのログデータ収集において、ログデータ中のエラーコードを抽出することにより、エラー状態のコンピュータからのログデータを優先的に送信するログデータ収集方式を開示する。また特開平5-280081号公報は、情報処理システムが障害ログを収集するとき貯蔵手段に貯蔵されたログ情報の個数が一定数に達したことを検出し、ログ記録の抑止を行うことにより重要な障害情報の消失を防ぐログ情報収集方式を開示する。また特開平3-111029号公報は、下位の設備端末からのデータが採取された時刻をデータに付与して上位の制御装置に送ることにより、複数の端末からの各データの時系列的な関係が図られることがないようにするデータ収集方式を開示する。

【0003】

【発明が解決しようとする課題】ネットワークを介して複数のコンピュータが接続され、コンピュータが他のコンピュータと通信しながら処理を遂げる分散処理システムにおいて、一人のユーザは複数の広範囲にわたるコンピュータやファイルにアクセスし得る。従ってログデータを解析することによってコンピュータやファイルの不正なアクセスを抽出するためには、個々のコンピュータが出力するログデータを中央のコンピュータに集約し、データベースに蓄積する必要がある。しかしながら各種のシステムプログラムやアプリケーションプログラムが出力するログデータは、各々そのデータ形式が異なっているため、単に個々のコンピュータプログラムが出力するログデータを収集して集約しただけではログデータの解析が困難である。また個々のコンピュータが保有する時刻がすべてのコンピュータに亘って一致しているとは限らないので、一般に個々のログデータに付与されている時刻にはずれが生じており、集約されたログデータを正しい時刻の順序に従って配列することが困難である。

【0004】本発明は、上記の事情に鑑みてなされたものであり、その目的とするところは、共通的なデータ形式に正規化されたログデータを管理することにある。

【0005】本発明の他の目的は、各サイトのコンピュータからログデータを収集する中央のコンピュータの時刻を基準とするログデータを管理することにある。

【0006】

【課題を解決するための手段】上記目的を達成するため、本発明は、監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成して蓄積する手段と、蓄積

された正規化ログデータをネットワークを介してマネージャの機能を実行するコンピュータへ送信する手段とをエージェントの処理手段として有するログデータの収集をするコンピュータを特徴とする。

【0007】また本発明は、ネットワークを介してエージェントの機能を実行するコンピュータからあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信する手段と、該正規化ログデータを補正時刻の順にデータベースに蓄積する手段とをマネージャの処理手段として有するログデータの収集と管理をするコンピュータを特徴とする。

【0008】

【発明の実施の形態】以下、本発明の一実施形態について図面に基づいて詳細に説明する。

【0009】図1は、本発明を適用する通信ネットワークの一例を示すシステム構成図である。ネットワークは複数のLAN1、3、4及びWAN（ワイド・エリア・ネットワーク）2に結合されるものである。マネージャ10は、計算機的主記憶装置に格納され、OSの下で実行するアプリケーションプログラム（AP）である。エージェント20は、サーバ等の計算機の主記憶装置に格納され、OSの下で実行するAPである。マネージャ10は、LAN1、3、4又はWAN2を介してエージェント20-1、20-2、20-3、20-4と通信することが可能である。図に示すように、エージェント20を実行する計算機はエージェント20と並行して他のAPを実行することが可能である。マネージャ10を実行する計算機もマネージャ10と並行して他のAPを実行することが可能であるが、充分なCPU性能と資源を確保するためには、専用の計算機を割り当てるのが望ましい。60はこのネットワークシステムを管理するネットワーク管理システムであり、ネットワーク管理プログラム及び図示しないネットワーク監視端末から構成される。ネットワーク管理システム60は、ネットワーク資源についての情報をマネージャ10に提供する。

【0010】図2は、マネージャとエージェントが行う処理動作の概略を示す図である。マネージャ10は、定義された各種ルールをエージェント20へ配布する（①）。エージェント20は、受信したルールを登録し、そのルールに従い監視対象ログファイル群30からログデータを入力し（②）、ログデータを正規化した後、正規化ログファイル40に格納する（③）。このとき正規化ログデータ中のログ出力時刻をマネージャ10の時刻を基準とする補正時刻によって補正する。エージェント20

は、マネージャ10からログ収集要求があったとき正規化ログファイル40から正規化されたログデータを取り出し（④）、マネージャ10へ転送する（⑤）。マネージャ10は、収集した正規化ログデータを補正時刻の順に正規化ログデータベース50に格納する（⑥）。またマネージャ10は、必要に応じて正規化ログデータベース50から任意の正規化ログデータを抽出し、その解析を行う。

【0011】図3は、マネージャ10の構成を示す機能ブロック図である。ルール110は定義された各種ルールであり、記憶装置に格納される。正規化ログデータベース50は、収集された正規化ログデータを格納するデータベースであり、記憶装置に格納される。ネットワーク管理システム60は、ネットワークを介してマネージャ10を格納する計算機と接続される他の計算機およびネットワークを監視する端末装置から構成されるシステムであり、マネージャ10と同じ計算機で実行するネットワーク管理プログラムは、ネットワークの構成要素である各通信回線、ルータ、中継機、各種計算機、計算機のプログラム等の動作状態（接続中、接続断、動作中、停止状態など）、各ネットワーク構成要素の所在場所などを管理する。以下マネージャ10を構成する各機能モジュールの機能の概要について述べる。

【0012】（1）ルール定義100

運用者が各種ルールを定義するためのプログラムツールであり、図示しない入力装置及び表示装置を介してユーザが容易にルールを設定できるようにGUI（グラフィカル・ユーザ・インタフェース）を提供する。

【0013】（2）スケジューラ101

ルール配布及びログ収集を実行する契機をそれぞれルール配布106及びログ収集107に知らせるプログラムである。契機の例として、例えば毎日午後5時、毎週土曜日の午後3時15分などのように実行開始を指示する。

【0014】（3）プロセス管理102

マネージャ10の100～109を付す各機能モジュールの起動/停止を制御するプログラムである。

【0015】（4）ログ解析103

データベース管理104を介して正規化ログデータベース50から正規化ログデータを抽出し、所定の解析を行うプログラムである。以下ログ解析がログデータである場合のログデータ解析の例を表1に示す。ログ事象及び正規化項目については後述する。

【0016】

【表1】

ログデータ解析の例(表1)

ログ解析項目	使用する正規化項目
規定のログイン地域でない所からログインし成功した	ユーザ名 接続元ホスト名 接続元IPアドレス
規定の時間外にログインして失敗した	ユーザ名 開始時刻
同一ユーザが別々の地域から同時にログインしている	ユーザ名 接続元ホスト名
一定期間に規定回数以上のログイン回数がありログインに失敗した	ログ事象 ログ事象結果 ユーザ名 補正時刻
規定回数以上、ユーザ名とパスワードの組み合わせを失敗したユーザ変更を行った	ログ事象 ログ事象結果 ユーザ名 変更後のユーザ名 補正時刻

【0017】(5) 構成管理104

対象とするエージェント20の機能を管理するプログラムである。またネットワーク管理システム60に問い合わせを行ってエージェント20が動作する計算機の動作有無やpingの応答時間等の情報を取得してルール配布106又はログ収集107に渡す。

【0018】(6) ルール管理105

ルール定義100から定義された各種ルールを受け取ってルール110に格納する。またルール110からルールを読み出してルール配布106に渡す。

【0019】(7) ルール配布106

スケジューラ101の指示に従い、ルール管理105から各種ルールを取得してエージェント20へ配布するプログラムである。

【0020】(8) ログ収集107

スケジューラ101の指示に従い、エージェント20から正規化ログファイルを収集するプログラムである。

【0021】(9) データ通信108

ルール配布106及びログ収集107がエージェント20と通信するときに通信制御を行うプログラムである。

【0022】(10) データベース管理109

ログ収集107がエージェント20から収集した正規化ログデータ群(正規化ログファイル)を正規化ログデータベース50に格納し、ログ解析103からの要求によって正規化ログデータを検索し抽出する。また所定の保存期間を過ぎた正規化ログデータを正規化ログデータベース50から削除し、未使用の記憶領域を生み出す。

【0023】図1は、エージェント20の構成を示す機能ブロック図である。ルール205は配布を受けた各種ルールであり、記憶装置に格納される。監視対象ログファイル群30は、監視対象とするログファイルであり、

記憶装置に格納される。正規化ログファイル40は、正規化ログデータを格納するファイルであり、記憶装置に格納される。以下エージェント20を構成する各機能モジュールの機能の概略について述べる。

【0024】(1) データ通信200

データ通信200は、ルール管理203及びログファイル管理204がマネージャ10と通信するときに通信制御を行うプログラムである。

【0025】(2) プロセス管理201

エージェント20の200~204を付す各機能モジュールの起動/停止を制御するプログラムである。

【0026】(3) ログ入力202

ルール管理203からログファイル監視ルールやフォーマットルール等を取得し、監視対象ログファイル群30から入力したログデータを正規化した後、正規化ログデータをログファイル管理204へ渡すプログラムである。

【0027】(4) ルール管理203

マネージャ10から配布された各種ルールをルール205として記憶装置に格納し、ログ入力202又はログファイル管理204の要求に応じてルールを提供するプログラムである。

【0028】(5) ログファイル管理204

ルール管理203からフィルタリングルールを取得し、ログ入力202から受け取った正規化ログデータをフィルタリングし、補正時刻を付加して正規化ログファイル40に格納する。マネージャ10のログ収集107から正規化ログファイル40の収集要求を受信したとき、正規化ログファイル40をマネージャ10へ転送する。

【0029】図5~図14は、正規化ログデータの構造の一例を示す図である。

【0030】図5は、正規化ログファイル40に格納される正規化ログデータ300の略略構成を示す図である。正規化ログデータ300は、共通情報クラス301と必要に応じて追加されるユーザ情報クラス302、サービス情報クラス303、アドレス情報クラス304、ファイル情報クラス305、トラフィック情報クラス306、個別情報クラス307等から構成される。共通情報クラス301は、すべての正規化ログデータ300に必須の情報クラスであり、残りの情報クラスは出力されたログデータに応じて選択されるものである。

【0031】図6は、共通情報クラス301のデータ構成を示す図である。正規化バージョン310は、正規化のバージョンを示す番号である。ログ種別はログ事象311、ログ事象結果312、ログ出力プログラム313、データ格納クラス314及びログファイル名315を含む。ログ出力プログラム313はログを出力したOS又はAPの名称であり、ログファイル名315はログ出力プログラム313が出力したログファイルの名称である。ログ事象311、ログ事象結果312及びデータ格納クラス314については後述する。マネージャは、マネージャを指称する計算機の名前316とホストIPアドレス317を格納する。エージェントは、ログを入力したエージェントを格納する計算機の名前318とホストIPアドレス319を格納する。監視対象は、監視対象とするサーバ等の計算機の名前320とホストIPアドレス321を格納する。時刻はログ出力時刻322と補正時刻323から成る。ログ出力時刻322はログを出力した計算機の局所的な時刻であり、補正時刻323はマネージャ10を格納する計算機の時刻に基づいて補正した時刻である。フィルタリングルール名324は、ログデータを正規化するときに応用したフィルタリングルールの名称である。

【0032】図7は、ユーザ情報クラス302のデータ構成を示す図である。ユーザ情報クラス302は、ログインしたユーザに関する情報を記録するものであり、ユーザ名330、ユーザID (UID) 331、ユーザ変更した後のユーザ名332、変更後のUID 333、ユーザのセキュリティレベル334、計算機やファイルへのアクセス権335、アクセスした結果336及びユーザが操作した端末装置の名称 (端末名337) を格納する。

【0033】図8は、サービス情報クラス303のデータ構成を示す図である。サービス情報クラス303は、ユーザに提供したサービスについての情報を記録する。サービスは、サービス名340、サービスバージョン341、サービス提供のために起動したプロセスの名称 (プロセス名342) 及びプロセスID 343を格納する。

【0034】図9は、アドレス情報クラス304のデータ構成を示す図である。アドレス情報クラス304は、

他計算機とコネクションを行ったときの情報を記録するものであり、接続元及び接続先のホスト名、IPアドレス、MACアドレス、ポート番号の他にコネクション状態、コネクションの開始時刻と終了時刻及び他計算機へのアクセス結果を格納する。

【0035】図10は、ファイル情報クラス305のデータ構成を示す図である。ファイル情報クラス305は、ユーザが作成又は変更したファイルについてファイル名、変更前のアクセス情報及び変更後のアクセス情報を記録する。アクセス情報は、ファイルの作成時刻、最終修正時刻、最終アクセス時刻、ファイルのinode (ノード) 番号、アクセス許可の有無、UID、グループID (GID) 及び最終的なファイルのサイズを格納する。

【0036】図11は、トラフィック情報クラス306のデータ構成を示す図である。トラフィック情報クラス306は、メール管理プログラム、ファイル転送プログラム等が出力するログ情報であり、ネットワークを介するデータやメッセージの受信バイト数、送信バイト数及びデータの転送時間 (処理時間) を記録する。

【0037】図12は、個別情報クラス307のデータ構成を示す図である。個別情報クラス307は、オプションであり、プログラムが出力するメッセージテキストの原文そのままの情報を記録する。

【0038】図13は、データ格納クラス314のデータ構成を示す図である。"T1" はデータ格納クラス314を識別するためのタグであり、"L1" は存在する情報クラスを指定する領域V1の長さを示す。"V1" は、各正規化ログデータ300に含まれる情報クラスを指定する領域であり、情報クラスの指定を開始するタグ、情報クラス識別子の長さ及び情報クラス識別子を順番に指定する。情報クラス識別子の長さは可変長である。各情報クラスを識別する番号をとすると、Tx (xは2) は情報クラスの開始を示すタグであり、Lx (xは2) はそのVxの部分の長さであり、Vx (xは2) は情報クラス識別子である。マネージャ10は、このデータ格納クラス314により各正規化ログデータを有する情報クラスを認識する。

【0039】図14は、正規化項目のうちコード化が可能なもののコード化テーブル600の一例を示す図である。正規化項目のログ事象311が"login"の場合はコード"1"に、ユーザ変更"su"の場合はコード"2"というようにコード化される。コネクト (connect) は、計算機間でファイル転送やプログラム間通信を行う際のコネクションに関するログ事象を示す。ファイルは内容が変更されたファイルに関するログ事象。ジョブはジョブの起動・停止・終了状態に関するログ事象である。メールはメール使用に関するログ事象を示す。ログ事象結果312はログ事象の結果であり、成功・失敗かを区別する。ユーザ情報クラス302のアクセス権335についてはあり/なしを区別する。ユー

サ情報クラス302及びアドレス情報クラス304のアクセス結果については、成功か失敗かを区分する。ファイル情報クラス305のアクセス許可については、ありなしを区分する。

【0040】図15〜図20は、ルールのデータ形式を示す図である。

【0041】図15は、マネージャールール450の一例を示す図である。DB...MAX451は正規化ログデータベース50が正規化ログデータを保存可能な期間を示す保存期間を定義する。RULE...MAX452はルール配布に使用できる最大の通信路数を定義する。LOG...MAX453はログ収集に使用できる最大の通信路数を定義する。ルール配布106やログ収集107は、この多重度数だけ通信路を使用できるが、処理の要求がこの多重度より大きい場合は通信路を順番に使用し、通信路が空くまで待った後、残りの処理を実行する。

【0042】図16は、エージェント20の動作条件ルール470の一例を示す図である。MANAGER...ADDRFSS471はマネージャのIPアドレスを定義し、FILE...MAXSIZE472は正規化ログファイル40が使用できる最大の記憶容量を定義する。

【0043】図17は、ログファイル監視ルール500の一例を示す図である。TARGET_LOG501は監視対象ログファイル名を定義し、FORMATによりファイルの形式（SEQ：シーケンシャル形式、WRAP：ラップアラウンド形式）を定義し、INTERVALにより監視間隔の時間（たとえば、10分間隔）を定義する。FMT_NAMEは当該ログファイルを正規化するときに応用するルールを定義する。例により説明すると、

TARGET_LOG=/usr/adm/syslog.log, FORMAT=SEQ, INTERVAL=10m, FMT_NAME=abc;

は、シーケンシャル形式のファイル/usr/adm/syslog.logを10分間隔で監視し、フォーマットルールabcにより正規化処理を行うことを示す。FMT_NAMEの指定がない場合は、エージェント20の間で共通のフォーマットルールにより正規化を行う。

【0044】図18と図19は、フォーマットルール510及び515の一例を示す図である。ログデータがテキスト形式の場合はFMT...Tを適用し、バイナリ形式の場合はFMT...Bを適用する。REGTEXT="文字列n"は、ログデータを選択する条件を示し、ログデータ中に文字列nが存在すれば、以下に示す規則に従ってログデータを正規化することを示す。&は論理積（AND）を示し、複数の文字列の存在を選択条件とすることができる。|はthenを意味し、以下ログデータの文字列のシーケンスに従って文字列から順に正規化項目を拾って行くことを意味する。正規化項目とは、各情報クラスで定義されるデータ項目のことである。:

は、ログデータの先頭から順番にポイントをずらして正規化項目に対応する値を切り出すための区切り文字である。正規化項目に就いて{|内に指定される文字は、任意のポイントから認識する文字列の長さ、またはその文字列が可変長の場合に認識する最後の文字を指定する。SKIPは、ログデータの先頭から順番にポイントをずらしていった場合、正規化項目に属さない文字列が存在する場合にその文字列を読み飛ばすことを意味し、{|内には読み飛ばす文字数又は認識する最後の文字となる"区切り文字"を指定する。{|区切り文字を指定した場合は、その区切り文字まで読み飛ばす。以下フォーマットルールの例を挙げる。

(a) フォーマットルールA

FMT,T:REGTEXT="SU" && REGTEXT=="+" | ログ事象=="2" | ログ事象結果=="0":SKIP[" "]; ログ出力時刻[10]:SKIP[3];端末名[" "]:ユーザ名[" "];変更後のユーザ名[" "];

(b) フォーマットルールB

FMT,T:REGTEXT=="connect" && REGTEXT=="refused" | ログ事象=="3" | ログ事象結果=="1":ログ出力時刻[15]:接続先ホスト名[" "]:プロセス名[" "]:プロセスID[" "]:SKIP["from "]:接続元ホスト名[" "];

図21は、ログファイルに格納されているメッセージテキストの原文の例を示す図である。メッセージテキスト551及び552は、OSが出力するユーザ変数に関するメッセージテキストの例である。メッセージテキスト553〜555は、OSがコネクション時に出力するメッセージテキストである。メッセージテキスト556及び557は、OSのジョブ管理が出力するメッセージテキストである。

【0045】メッセージテキスト551をフォーマットルールAによって正規化すると、

- ・ログ事象311=2 (su)
- ・ログ事象結果312=0 (成功)
- ・ログ出力時刻322=1'30 11:18のエポックタイム
- ・端末名337=typ5
- ・ユーザ名330=funio
- ・変更後のユーザ名332=root

となる。

【0046】メッセージテキスト554をフォーマットルールBによって正規化すると、

- ・ログ事象311=3 (connect)
- ・ログ事象結果312=1 (失敗)
- ・ログ出力時刻322=Jan 12 13:12:15のエポックタイム
- ・接続先ホスト名354=hosta
- ・接続先IPアドレス355=hostaをIPアドレスに変換した値

・プロセス名 342=fipd
 ・プロセスID 343=1111
 ・接続元ホスト名 350=hostb
 ・接続元IPアドレス 351=hostbをIPアドレスに変換した値となる。

【0047】図20は、フィルタリングルール520の一例を示す図であり、ログファイル管理204が該当する正規化ログデータだけを格納するためのルールである。D.L.Tはフィルタリングルールであることを示し、正規化項目が指定した文字列やコードであったり、指定した時間帯の正規化ログデータであった場合、そのような条件に適合する正規化ログデータだけを抽出して格納する。==はイコールを、!=はnotイコールを、&は論理積ANDを、||は論理和ORを、—は時間間隔をそれぞれ意味する。

【0048】図22は、正規化ログデータベース50のデータ構造を例示する図である。正規化ログデータベース50は、正規化ログデータを補正時刻630の順に配列して格納する。ある補正時刻630から其通報クラス631のログデータにチェーンする。また其通報クラス631からこれに続いて存在する情報クラスのログデータに次々とチェーンする。情報クラスに対応して示される検索キーは、正規化ログデータを検索するときキーとして使用される正規化項目を示すものである。また補正時刻630から次の補正時刻630へチェーンが張られている。ユーザは、補正時刻630によって、また該当する情報クラスを検索キーを指定することによって正規化ログデータベース50から目的とする正規化ログデータを効率良く抽出することができる。

【0049】図23は、マネージャ10のルール配布106の処理の流れを示すPAD図である。ルール配布106は、初期設定(ステップ701)後、プロセス管理102から終了要求が来るまでループし(ステップ702)、イベントを持つ(ステップ703)。イベントには、スケジューラ101からのルール配布要求(ステップ704)とプロセス管理102からの終了要求(ステップ712)がある。

【0050】ルール配布要求(ステップ704)を受信した場合は、ルール管理105を介して配布するルールと配布先であるエージェント20の一覧を取得し(ステップ705)、構成管理104からエージェント20の動作状態及び応答時間の情報を取得する(ステップ706)。取得したエージェント20のping応答時間を応答時間の小さい順番に並び替える(ステップ707)。このとき動作していないエージェント20については、応答時間を無限大と解釈する。ルールを配布するエージェント20の数だけループし(ステップ708)、エージェント20が動作している場合(ステップ709YES)は応答時間の小さい順番にルールを配布

し(ステップ710)、エージェント20が動作していない場合はルール配布失敗のメッセージを出力する(ステップ711)。ルール配布に当っては、RULE_MAX 452を適用する。配布したルールは、エージェント20のルール管理203に転送される。

【0051】終了要求を受信した場合は(ステップ712)、ループを抜けて終了処理を行う(ステップ713)。

【0052】図24は、マネージャ10のログ収集107の処理の流れを示すPAD図である。ログ収集107は、初期設定(ステップ801)後、プロセス管理102から終了要求が来るまでループし(ステップ802)、イベントを持つ(ステップ803)。イベントには、スケジューラ101からのログ収集要求(ステップ804)、エージェント20からの起動通知(ステップ811)、及びプロセス管理102からの終了要求(ステップ816)がある。

【0053】ログ収集要求を受信した場合は(ステップ804)、スケジューラ101からログを収集するエージェント20の一覧を取得し(ステップ805)、構成管理104からこれらのエージェント20の動作状態及び応答時間の情報を取得するとともに、応答時間の短い順番にエージェント20をソートする(ステップ806)。ログを収集するエージェント20の数だけループし(ステップ807)、エージェントが動作している場合(ステップ808YES)はログを収集し(ステップ809)、エージェントが動作していない場合(ステップ808NO)はログ収集失敗メッセージを出力する(ステップ810)。ログ収集に当っては、LOG_MAX 453を適用する。ログ収集107は、エージェント20のログファイル管理204を介して正規化ログファイル40を収集する。

【0054】エージェント起動通知を受信した場合は(ステップ811)、構成管理104からエージェント20とのping(ICMPエコーリクエスト)の応答時間を取得する(ステップ812)。ICMP(Internet Control Message Protocol)は、通信ネットワークの管理に際する国際的な標準規格の1つであるアイ・エイ・ビー(IAB:Internet Activities Board)の管理標準である。ICMPを使用すると、IPノード(例えばコンピュータ)が他のIPノードと通信可能であるか否かを確認できる。またpingを使用すると、任意のIPノードと通信可能であるか否かの動作状態と応答時間を取得できる。ping応答時間を取得できた場合(ステップ813YES)は、マネージャ10の現在時刻にこの応答時間から得られる通信時間を加算した時刻を起動通知を発行したエージェント20へ通知する(ステップ814)。マネージャの時刻にマネージャから伝えるためには、マネージャの時刻にマネージャから

エージェントへの通信時間を加えた時刻を通知すればよい。pingの応答時間は、マネージャからエージェントとエージェントからマネージャ、つまり行きと返りの通信時間を加えた時間間隔である。そこでping応答時間の1/2を通信時間として利用する。すなわちマネージャは、次の計算式によりエージェントの時刻を推定しエージェントへ通知する。

(エージェントの時刻) \approx (マネージャの時刻) + (ping応答時間) / 2

応答時間を取得できなかった場合(ステップ813N)の、すなわちネットワーク管理システム60から情報を得られない場合は、単にマネージャ10の現在時刻をエージェント20へ通知する(ステップ815)。エージェント20は、マネージャ10の現在時刻を取得して正規化ログデータの補正時刻523に適用する。

【0055】終了要求を受信した場合は(ステップ816)、ループを抜けて終了処理を行う(ステップ817)。

【0056】図25は、マネージャ10の構成管理104の処理の流れを示すPAD図である。構成管理104は、初期設定(ステップ901)後、プロセス管理102から終了要求が来るまでループし(ステップ902)、イベントを持つ(ステップ903)。イベントにはルール配布106からのエージェント情報格納要求(ステップ904)、ルール配布106やログ収集107からのエージェント情報取得要求(ステップ909)と、プロセス管理102からの終了要求(ステップ913)がある。

【0057】エージェント情報格納要求を受信した場合は(ステップ904)、ルール配布106からルールを配布したエージェント20の情報を取得する(ステップ905)。エージェント20の情報とは、ルールの配布時刻、配布したルール名などである。ネットワーク管理システム60と通信可能であるとき(ステップ906YES)は、取得したエージェント情報をネットワーク管理システム60に送す(ステップ907)。ネットワーク管理システム60は、受信したルール配布の履歴情報をネットワーク管理のために利用可能である。ネットワーク管理システム60と通信できないとき(ステップ906NO)は、エージェント情報を構成管理104に保存するファイルへ格納する(ステップ908)。

【0058】エージェント情報取得要求を受信した場合は(ステップ909)、ネットワーク管理システム60と通信できるとき(ステップ910YES)には、ネットワーク管理システム60からエージェント20の、動作有無やpingの応答時間等を取得しこれらの情報を要求元に送す(ステップ911)。ネットワーク管理システム60と通信できないとき(ステップ910NO)には、構成管理104のファイルからエージェントの履歴についての情報を取得して要求元に送す(ステ

ップ912)。

【0059】終了要求を受信した場合は(ステップ913)、ループを抜けて終了処理(ステップ914)を行う。

【0060】図26は、マネージャ10のデータベース管理108の処理の流れを示すPAD図である。データベース管理108は、初期設定(ステップ1001)し、正規化ログデータベース50に格納している正規化ログデータの保存期間の確認を要求(ステップ1002)した後、プロセス管理102から終了要求が来るまでループし(ステップ1003)、イベントを持つ(ステップ1004)。イベントには、ログ収集107からの正規化ログデータ格納通知(ステップ1005)、ログ解析103からの正規化ログデータ抽出要求(ステップ1008)、データベース管理108自身から正規化ログデータの保存期間を確認するための要求(ステップ1010)と、プロセス管理102からの終了要求(ステップ1014)がある。

【0061】正規化ログデータ格納通知を受けた場合は(ステップ1005)、ログ収集107から正規化ログデータを取得し正規化ログデータベース50に格納する(ステップ1006)。格納に当たっては、図22のデータ構造に従って正規化ログデータを格納する。正規化ログデータは補正時刻630の順に配列されるので、この順に従って正規化ログデータをマージする。また正規化ログデータの保存期間確認を要求する(ステップ1007)。

【0062】正規化ログデータ抽出要求を受信した場合は(ステップ1008)、指定された検索キーにより正規化ログデータベース50を検索し、その結果抽出したデータを要求元へ応答する(ステップ1009)。

【0063】保存期間確認要求(ステップ1010)を受信した場合は、正規化ログデータベース50に格納されている正規化ログデータの一番古い補正時刻630と現在時刻の差と、DB_MAX451とを比較し(ステップ1011)、保存期間より古い正規化ログデータを保存しているときは古い正規化ログデータを削除し(ステップ1012)、利用者に知らせるために音響メッセージを出力する(ステップ1013)。

【0064】終了要求を受信した場合は(ステップ1014)、ループを抜けて終了処理(ステップ1015)を行う。

【0065】図27は、エージェント20のログ入力202の処理の流れを示すPAD図である。ログ入力202は、初期設定し(ステップ1101)、エージェント20のルール管理203からログファイル参照ルール500とフォーマットルール510、515書を取得(ステップ1102)後、プロセス管理201から終了要求が来るまでループし(ステップ1103)、イベントを持つ(ステップ1104)。イベントには、ログファイ

ル管理204からのログ入力中断要求(ステップ1105)とログ入力再開要求(ステップ1107)、プロセス管理201からの終了要求(ステップ1109)及び時間監視によるタイマ割り込みがある。

【0066】ログ入力中断要求を受信した場合は(ステップ1105)、ログ入力を中断する(ステップ1106)、中断する要因は、正規化ログファイル40の容量がFILLER_MAXSIZE47に達したときである。

【0067】ログ入力再開要求を受信した場合は(ステップ1107)、ログ入力を再開する(ステップ1108)。再開する要因は、正規化ログファイルをマネージャ10へ転送したときである。

【0068】終了要求を受信した場合は(ステップ1109)、ループを抜けて終了処理(ステップ1117)を行う。

【0069】ログファイル監視ルール500に設定された監視期間に従ってログファイルの監視時刻になったとき、監視対象ログファイル群30をオープン(ステップ1111)、このログファイルのファイル管理情報を取得する。ファイル管理情報が前回取得したものと同じか否かを検証する(ステップ1112)。同じ場合は(ステップ1112YES)、前回オープンしたファイルと同じ内容であるため前回のファイルのオフセットからログデータを入力する(ステップ1113)。前回のファイルのオフセットは、当該ファイルについて前回入力済のレコードの次のレコードを指している。異なる場合は(ステップ1112NO)、新しいファイル(前回オープンしたファイルは削除された等)であると解釈し、先頭からログデータを入力する(ステップ1114)。その後、入力したログデータを正規化し(ステップ1115)、正規化ログデータをログファイル管理204へ通知する(ステップ1116)。ログデータの正規化は、上記のようにフォーマットルール510、515等を用いて行う。正規化ログデータをログファイル管理204に通知した後、当該ログファイルをクローズし、監視期間に従って次の監視時刻にタイマを設定する。

【0070】図28は、エージェント20のログファイル管理204の処理の流れを示すフロー図である。ログファイル管理204は、初期設定し(ステップ1201)、ルール管理203から動作条件ルール470とフィルタリングルール520を取得(ステップ1202)した後、プロセス管理201から終了要求が来るまでループし(ステップ1203)、イベントを持つ(ステップ1204)。イベントには、ログ入力202からの正規化ログデータ格納通知(ステップ1205)、マネージャ10のログ収集107からのログ収集要求(ステップ1209)、ログファイル管理204自身からの正規化ログファイル容量確認要求(ステップ1211)、マネージャ10のログ収集107からのマネージャ時刻の

通知(ステップ1216)と、プロセス管理201からの終了要求(ステップ1218)がある。

【0071】正規化ログデータ格納通知を受信した場合は(ステップ1205)、ログ入力202から正規化ログデータを取得し(ステップ1206)、エージェントとマネージャの時間差(ステップ1217の処理結果)とログ出力時刻322から補正時刻323を計算する。ログ入力202から取得した正規化ログデータにこの補正時刻323を追加して正規化ログファイル40に格納する(ステップ1207)。取得した正規化ログデータにフィルタリングルール520を適用して条件に合致する正規化ログデータのみを正規化ログファイル40に格納する、次に正規化ログファイル容量確認要求を発行する(ステップ1208)。

【0072】ログ収集要求を受信した場合は(ステップ1209)、正規化ログファイル40中の正規化ログデータを補正時刻323の順にソートした後、MANAGER_ADDRESS471に示されるマネージャ10へ転送する(ステップ1210)。

【0073】正規化ログファイル容量確認要求を受信した場合は(ステップ1211)、正規化ログファイルの使用容量とFILLER_MAXSIZE47とを比較し(ステップ1212)、最大サイズに達したとき(ステップ1212YES)は、ログ入力202へ中断通知を発行する(ステップ1213)。最大サイズに達していないとき(ステップ1212NO)は、前回中断要求を発行したか確認し(ステップ1214)、発行していたとき(ステップ1214YES)は、ログ入力202へログ入力再開要求を通知する(ステップ1215)。

【0074】マネージャ時刻の通知を受信した場合は(ステップ1216)、エージェントとマネージャのコンピュータ時刻の差を計算する(ステップ1217)。

【0075】終了要求を受信した場合は(ステップ1218)、ループを抜けて終了処理(ステップ1219)を行う。

【0076】

【発明の効果】以上説明したように本発明によれば、エージェントが複数のログデータを監視し種々の形式で出力されたログデータを入力した後、正規化を行い共通的なデータ形式に変換する。また必要なログデータだけを抽出し、ログデータの出力時刻としてマネージャの時刻に合わせた補正時刻を使用するようにしたので、利用者はネットワークに存在する複数のコンピュータのログデータを統一したデータ形式及び時刻に基づいて解析することができる。

【0077】またマネージャが蓄積するログデータについては、所定期間のログデータを保存するようにしたので、古いログデータから漸に削除する形でログ情報の容量を規制できる。

【0078】さらに収集したログデータを補正時刻及び

正規化項目によって検索可能としたので、運用者は必要なログ情報を容易に取得できる。

【図面の簡単な説明】

【図1】実施形態のネットワークシステムの構成図である。

【図2】実施形態のマネージャとエージェントが行う処理動作の概略を示す図である。

【図3】実施形態のマネージャ10の構成を示す機能ブロック図である。

【図4】実施形態のエージェント20の構成を示す機能ブロック図である。

【図5】実施形態の正規化ログデータの概略構成を示す図である。

【図6】実施形態の共通情報クラスのデータ構成を示す図である。

【図7】実施形態のユーザ情報クラスのデータ構成を示す図である。

【図8】実施形態のサービス情報クラスのデータ構成を示す図である。

【図9】実施形態のアドレス情報クラスのデータ構成を示す図である。

【図10】実施形態のファイル情報クラスのデータ構成を示す図である。

【図11】実施形態のトラフィック情報クラスのデータ構成を示す図である。

【図12】実施形態の個別情報クラスのデータ構成を示す図である。

【図13】実施形態のデータ格納クラスのデータ構成を示す図である。

【図14】正規化項目のコード化テーブルの例を示す図である。

【図15】マネージャールの例を示す図である。

【図16】エージェントの動作条件ルールの例を示す図

である。

【図17】エージェントのログファイル監視ルールの例を示す図である。

【図18】エージェントのフォーマットルール（その1）の例を示す図である。

【図19】エージェントのフォーマットルール（その2）の例を示す図である。

【図20】エージェントのフィルタリングルールの例を示す図である。

【図21】監視対象ログファイルのログデータであるメッセージテキストの例を示す図である。

【図22】実施形態の正規化ログデータベースのデータ構造を示す図である。

【図23】実施形態のマネージャが行うルール配布の処理の流れを示すP A D図である。

【図24】実施形態のマネージャが行うログ収集の処理の流れを示すP A D図である。

【図25】実施形態のマネージャが行う構成管理の処理の流れを示すP A D図である。

【図26】実施形態のマネージャが行うデータベース管理の処理の流れを示すP A D図である。

【図27】実施形態のエージェントが行うログ入力の処理の流れを示すP A D図である。

【図28】実施形態のエージェントが行うログファイル管理の処理の流れを示すP A D図である。

【符号の説明】

10・・・マネージャ、20・・・エージェント、40・・・正規化ログファイル、50・・・正規化ログデータベース、60・・・ネットワーク管理システム、104・・・構成管理、106・・・ルール配布、107・・・ログ収集、109・・・データベース管理、110・・・ルール、202・・・ログ入力、204・・・ログファイル管理、205・・・ルール

【図7】

図 7

ユーザ情報クラス ～302

ユーザ名	～330
UID	～331
変更後のユーザ名	～332
変更後のUID	～333
セキュリティレベル	～334
アクセス権	～335
アクセス結果	～336
端末名	～337

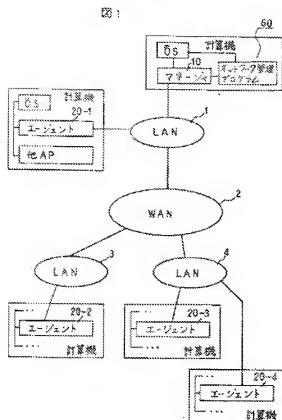
【図8】

図 8

サービス情報クラス ～303

サービス名	～340
サービスバージョン	～341
プロセス名	～342
プロセスID	～343

【図1】



【図11】

図 1 1

トラフィック情報クラス ~306

受信バイト数
送信バイト数
処理時間

【図12】

図 1 2

個別情報クラス ~307

メッセージテキスト

【図5】

図 5

正規化ログデータ

~300

共通情報クラス	~301
ユーザ情報クラス	~302
サービス情報クラス	~303
アドレス情報クラス	~304
ファイル情報クラス	~305
.	
.	
トラフィック情報クラス	~306
個別情報クラス	~307

【図6】

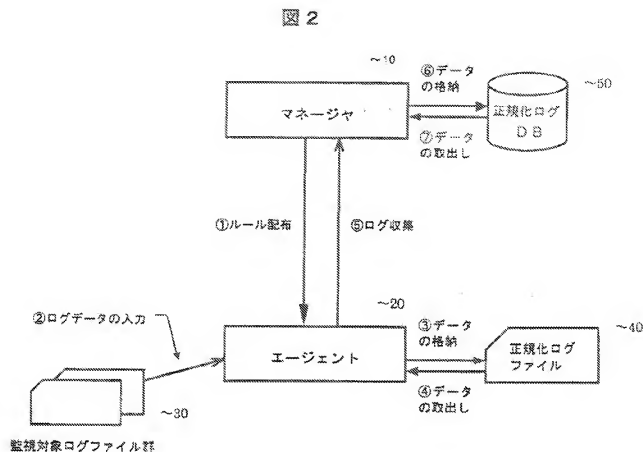
図 6

共通情報クラス

~301

正規化バージョン		~310
ログ種別	ログ事象	~311
	ログ事象結果	~312
	ログ出力プログラム	~313
	データ格納クラス	~314
	ログファイル名	~315
マネージャ	ホスト名	~316
	ホストIPアドレス	~317
エージェント	ホスト名	~318
	ホストIPアドレス	~319
監視対象	ホスト名	~320
	ホストIPアドレス	~321
時刻	ログ出力時刻	~322
	補正時刻	~323
フィルタリングルール名		~324

【図2】



【図9】

図9 アドレス情報クラス ～304

接続元ホスト名	～350
接続元IPアドレス	～351
接続元MACアドレス	～352
接続元ポート番号	～353
接続先ホスト名	～354
接続先IPアドレス	～355
接続先MACアドレス	～356
接続先ポート番号	～357
コネクション状態	～358
開始時刻	～359
終了時刻	～360
アクセス結果	～361

【図15】

図15 マネージャルール ～430

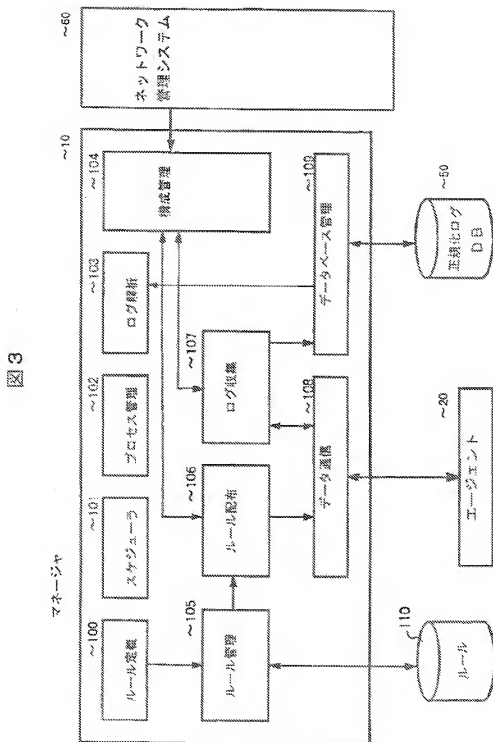
DB_MAX: 正規化ログデータの保存期間;	～431
RULE_MAX: ルール配布の最大数;	～432
LOG_MAX: ログ収集の最大数;	～433

【図16】

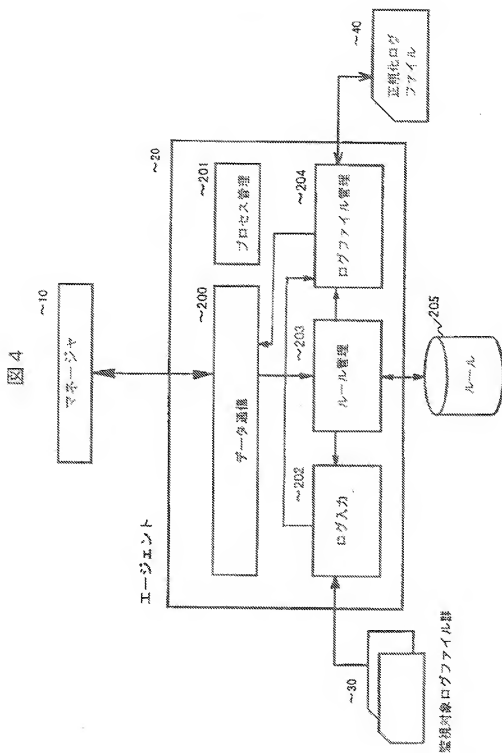
図16 エージェントルール ～470

MANAGER_ADDRESS: マネージャのIPアドレス;	～471
FILE_MAXSIZE: 正規化ファイルの最大サイズ;	～472

【243】



【図4】



【図10】

【図13】

図10

ファイル情報クラス

～305

ファイル名	
変更後	作成時刻
	最終修正時刻
	最終アクセス時刻
	i-node番号
	アクセス許可
	UID
	GID
	サイズ
変更前	作成時刻
	最終修正時刻
	最終アクセス時刻
	i-node番号
	アクセス許可
	UID
	GID
	サイズ

図13

データ格納クラス

～314

T1	L1	V1 (存在する情報クラスの指定領域)					
		T2	L2	V2	T5	L5	V5
						

【図18】

図18

フォーマットルール (その1)

～510

```

PUT_1: REGTEXT == "文字列1" | ログ番号 == "1" | ログ事象結果 == "0"
正規化項目1[文字数]、正規化項目2[終了文字]、...;
PUT_2: REGTEXT == "文字列2" AND REGTEXT == "文字列3" | ログ番号 == "0"
| ログ事象結果 == "1"、正規化項目1[終了文字]、DUP[既知/未知/文字数]、
正規化項目4[文字数]、...;

```

【図19】

図19

フォーマットルール (その2)

～545

```

PUT_3: REGTEXT == "文字列0" AND REGTEXT == "文字列0" | ログ番号 == "2"
| ログ事象結果 == "1"、正規化項目1[終了文字]、DUP[既知/文字数]、正規
化項目3[文字数]、...;

```

【図17】

図17

ログファイル監視ルール

～500

```

TARGET_LOG: "監視対象ログファイル名1", FORMAT=REG, INTERVAL=時間;
PUT_NAME: フォーマットルール名;
FORGET_LOG: "監視対象ログファイル名2", FORMAT=WRAP, INTERVAL=時間;

```

【図21】

図21

メッセージテキスト例

～550

```

30 01/30 11:10 + tty05 fujin-vant ~551
30 01/31 11:52 + tty07 morita-sbo ~552
Jan 4 12:38:10 hosta fipd[111]: connect from 170.213.252.12 ~553
Jan 12 12:17:15 hosta fipd[111]: fipd[111] connect from hosta ~554
Jan 18 15 10:05 hosta. #too[7777]: connect to hosta ~555
Jan 25 10 12 34 hosta job[2222]: ジョブABCを削除しました。 ~556
Jan 29 10 15:10 hosta job[2222]: ジョブABCが既削除しました。 ~557

```

【図20】

図20

フィルタリングルール

～530

```

L1: 正規化項目1 == "文字列1";
L2: 正規化項目2 == "文字列2" | 正規化項目3 == "文字列3";
L3: 正規化項目4 == "文字列4" AND 正規化項目5 == "文字列5";
L4: 正規化項目6 == "時刻1" AND 時刻2 == "時刻2" AND 正規化項目7 == "文字列7";

```


【図14】

図14

正規化項目のコード化テーブル

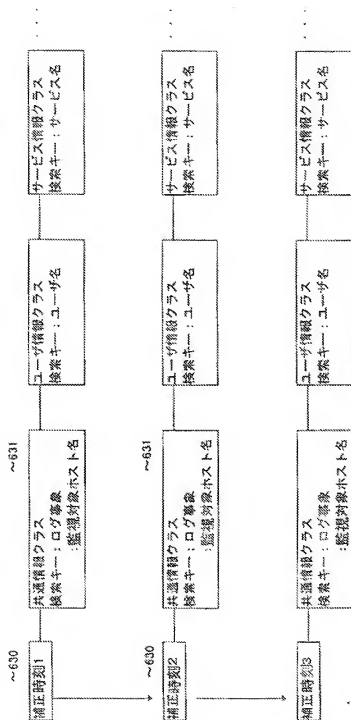
～600

正規化項目	内容	コード
ログ事象	login	1
	su (ユーザ変更)	2
	connect	3
	ファイル	4
	ジョブ	5
	メール	6
ログ事象結果	成功	0
	失敗	1
アクセス権	あり	0
	なし	1
アクセス結果	成功	0
	失敗	1
アクセス許可	あり	0
	なし	1

【図22】

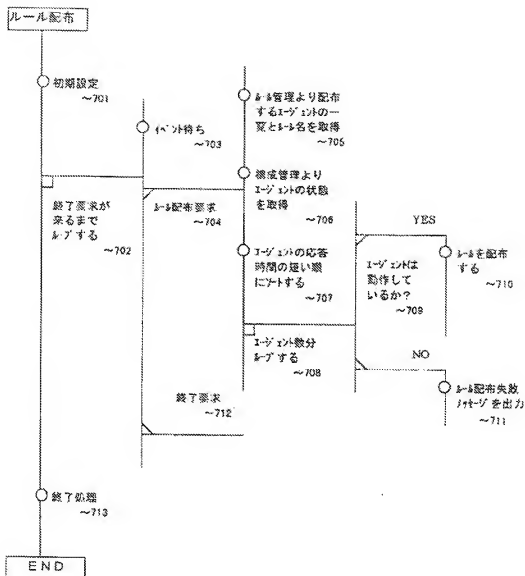
図 22

50: 正規化ログデータベース



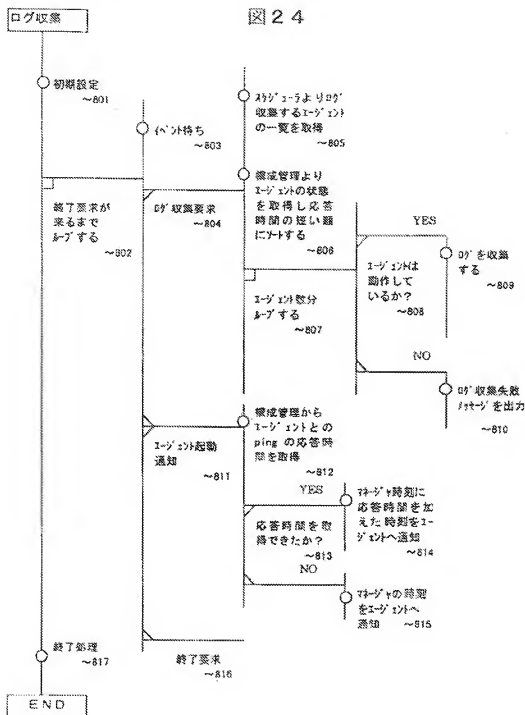
【図 23】

図 23



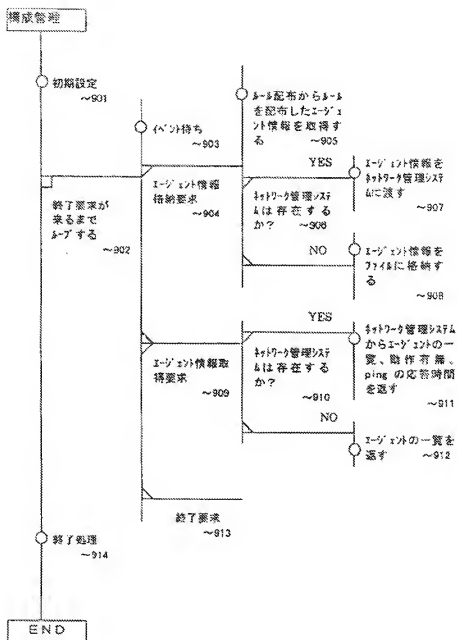
【図24】

図 24



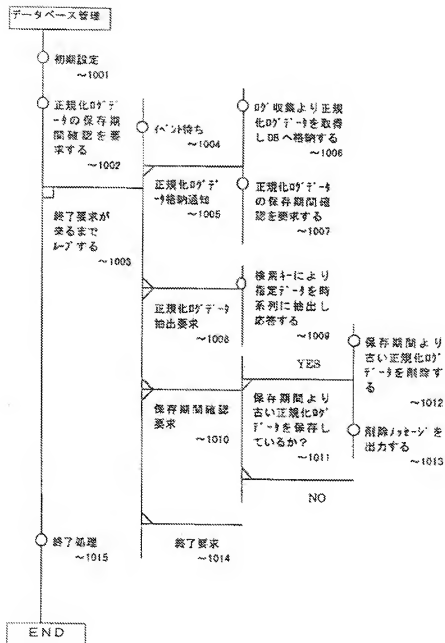
【図25】

図 25



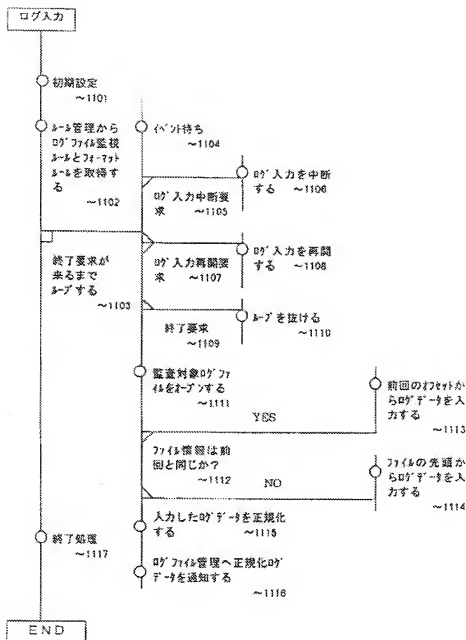
【図26】

図 26



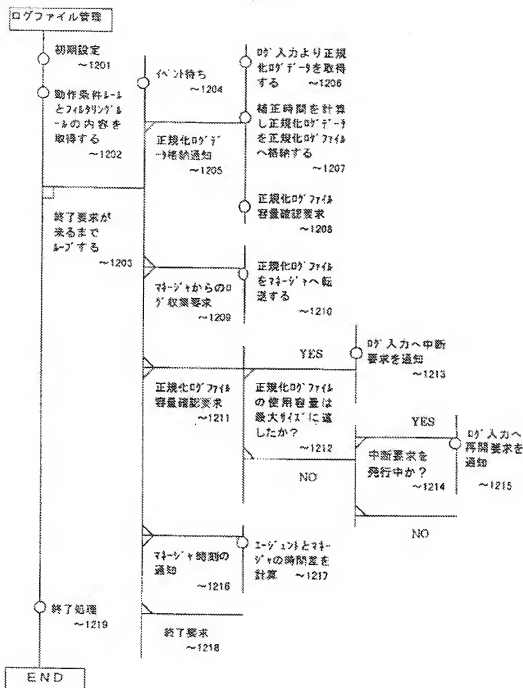
【図27】

27



【図28】

28



フロントページの続き

(72)発明者 中野 秀紀

東京都千代田区大手町二丁目6番2号 株
式会社日立情報ネットワーク内

(72)発明者 森田 眞司

神奈川県横浜市中区磯子区磯子5030番地 株
式会社日立製作所ソフトウェア開発本部内

(72)発明者 山田 資

神奈川県横浜市中区戸塚町5030番地 株
式会社日立製作所ソフトウェア開発本部内

(72)発明者 新村 美貴

神奈川県横浜市中区戸塚町5030番地 株
式会社日立製作所ソフトウェア開発本部内

Computer use meter and analyzer

Publication number: JP10510647 (T)

Publication date: 1996-10-13

Inventor(s):

Applicant(s):

Classification:

- International: G06F1/00; G06F11/34; G06F13/00; G06F15/00; G06F21/00; H04Q9/00; IPC1-7; G06F11/34; G06F13/00; H04Q9/00

- European: G06F11/34; G06F21/00; G06F13/00; H04Q9/00

Application number: JP19950502197T 19950607

Priority number(s): WO1995US10091 19950807, US19950474022 19950607

Also published as:

US6115680 (A)

US5675510 (A)

WO9641495 (A1)

NO975728 (A)

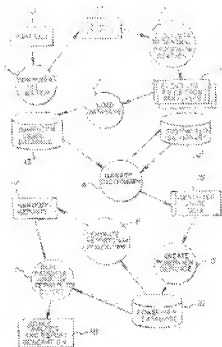
MX9708752 (A)

FIG. 1

Abstract not available for JP 10510647 (T)

Abstract of corresponding document, US 5115680 (A)

PCT No. PCT/US96/10091 Sec. 371 Date Mar. 2, 1996 Sec. 102(a) Date Mar. 2, 1996 PCT Filed Jun. 7, 1995 PCT Pub. No. WO95/41495 PCT Pub. Date Dec. 19, 1995 The subject system measures and reports the use of a personal computer by a user through a log file. The log file includes entries corresponding to predetermined events and can report on the applications used and communication functions engaged in by the user. The log files from one or more computers may be assembled and analyzed in order to ascertain computer use habits for computer software, computer hardware and computer communications. The system may also be used to predict computer use trends and to represent computer use history.



Data supplied from the **espacenet** database — Worldwide

特表平10-510647

(43) 公表日 平成10年(1998)10月13日

(51) Int. Cl. ⁵	観別記号	F I
G 0 6 F 11/34		G 0 6 F 11/34 C
13/00	3 5 4	13/00 3 5 4 D
H 0 4 Q 9/00	3 0 1	H 0 4 Q 9/00 3 0 1 B
	3 1 1	3 1 1 H

審査請求 有 予備審査請求 有 (全 30 頁)

(21) 出願番号 特願平9-502197
 (86) (22) 出願日 平成8年(1996)6月7日
 (85) 国際文提出日 平成9年(1997)12月8日
 (86) 国際出願番号 PCT/US96/10091
 (87) 国際公開番号 WO96/41495
 (87) 国際公開日 平成8年(1996)12月19日
 (31) 優先権主張番号 08/474,082
 (32) 優先日 1995年6月7日
 (33) 優先権主張国 米国 (US)

(71) 出願人 メディア・メトリックス・インコーポレーテッド
 アメリカ合衆国、ニューヨーク州
 11050、ポート・ワシントン、ウエスト・
 ショアー・ロード 900
 (72) 発明者 コフィー、 スティーブン・アール
 アメリカ合衆国、ニューヨーク州
 11837、イースト・ハンプトン、スプリングス・フィアープレイス・ロード 487
 (74) 代理人 弁理士 鈴江 武彦 (外4名)

最終頁に続く

(54) 【発明の名称】 コンピュータ使用メーターおよび解析装置

(57) 【要約】

本発明のシステムは、ログファイル(11)を通してユーザーによるパーソナルコンピュータの使用量を測定して報告する。ログファイル(11)は、予め定められた事象に対応した項目を含み、使用されたアプリケーション、およびユーザーがたずさわった通信機能において報告することができる。1以上のコンピュータからのログファイル(11)は、コンピュータソフトウェア、コンピュータハードウェア、およびコンピュータ通信に対するコンピュータ使用の性質を確認するために収集され、解析されてもよい。システムはまた、コンピュータ使用傾向を予測し、またコンピュータ使用履歴を表すために使用されてもよい。

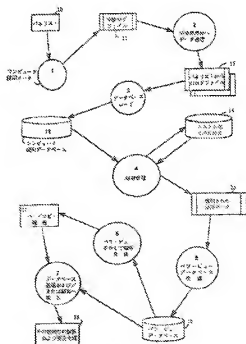


Figure 1

【特許請求の範囲】

1. ユーザー・コンピュータ・マシン中に設置され、前記コンピュータ・マシンのメモリに記憶された予め定められたマシン動作事象のログをそれぞれ含んでいく複数のローカル・コンピュータ使用メーターと、

コンピュータ・マシン中に設置され、予め定められたマシン動作事象のログをコンピュータ・メモリにロードする処理ステーションと、

コンピュータ・マシン中に設置され、前記コンピュータ・マシンのメモリに記憶されたマシン動作事象に基づいてアクセス、処理および報告の作成をするように構成されたデータベース管理システムとを含んでおり、

前記処理ステーションが、前記複数のローカル・コンピュータ使用メーターにリンクされているコンピュータ使用監視システム。

2. 前記処理ステーションは、電子通信チャンネルによって前記複数のローカル・コンピュータ使用メーターにリンクされている請求項1記載のコンピュータ使用監視システム。

3. 前記電子通信チャンネルは、予め定められた基準に基づいて設定されている請求項2記載のコンピュータ使用監視システム。

4. 前記予め定められた基準は周期的である請求項3記載のコンピュータ使用監視システム。

5. 前記予め定められた基準は、前記ログによって占有されたメモリの量に基づいている請求項3記載のコンピュータ使用監視システム。

6. 前記処理ステーションは、ユーザーコンピュータマシンから可搬性媒体に記録を転送する手段と、可搬性媒体から処理ステーションに前記記録を転送する手段とによって前記複数のローカル・コンピュータ使用メーターにリンクされる請求項1記載のコンピュータ使用監視システム。

7. 前記予め定められたマシン動作事象は、オペレーティングシステムのコール・バック・メッセージに対応した事象を含んでいる請求項1記載のコンピュータ使用監視システム。

8. 前記予め定められたマシン動作事象は、受取られたモデム文字ストリングに対応した事象を含んでいる請求項1記載のコンピュータ使用監視システム。

9. さらに、前記処理ステーションと関連したコンピュータメモリに記憶された辞書ファイルと、

ログファイルに書込まれたマシン動作事象を辞書ファイルを参照することによって解釈する手段とを含んでいる請求項1記載のコンピュータ使用監視システム。

10. オペレーティングシステム・メッセージを傍受して、オペレーティングシステム・メッセージモジュールに応答する予め定められたタイプのメッセージの受信を示し、

選択されたオペレーティングシステム・メッセージに応答する事象ログを作成および記憶し、

1以上のコンピュータシステムから中央システムに1以上の事象ログを転送し、

前記事象ログの内容を解析するステップを含んでいるコンピュータの使用監視方法。

11. 複数の各ユーザー使用コンピュータシステムにおいて多数のマシン動作事象を生成し、

前記ユーザーコンピュータシステムのローカル・コンピュータメモリ中のログに各事象を記憶し、

前記ユーザーコンピュータシステムから処理ステーションコンピュータに前記記憶された事象を転送し、

前記処理ステーションコンピュータと関連したメモリに前記事象ログをロードし、

前記処理ステーションコンピュータと関連したメモリに記憶された辞書を参照することによって前記事象ログを解釈し、

前記解釈されたコンピュータ事象ログを特定の基準にしたがって編集および報告するステップを含んでいる複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

12. 前記転送するステップは、電子通信チャンネルを介して行われる請求項11記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定

する方法。

13. 前記転送するステップは、予め定められた基準に基づいて開始される請求

項12記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

14. 前記予め定められた基準は、周期的である請求項13記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

15. 前記予め定められた基準は、前記ログによって占有されたメモリの量に基づいている請求項13記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

16. 前記転送するステップは、ユーザーコンピュータマシンから可搬性磁気媒体に記録を転送して、前記可搬性磁気媒体から前記処理ステーションコンピュータに前記記録を転送する請求項11記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

17. 前記マシン動作事象は、オペレーティングシステム・コールバック・メッセージに対応した予め定められた事象を含んでいる請求項11記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

18. 前記マシン動作事象は、傍受されたモデム文字ストリングに対応した事象を含んでいる請求項11記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

19. コンピュータモニタ上に表示された情報を周期的に監査し、

使用活動を示すラベルのログを作成および記憶するステップを含んでいるコンピュータ使用監視方法。

20. 前記監査するステップは、予め選択されたコンピュータ・アプリケーション・プログラムによって表示された情報をポーリングでチェックする請求項19記載のコンピュータ使用監視方法。

21. 前記予め選択されたコンピュータアプリケーション・プログラムは、オンラインサービス・アクセスおよびインターフェイス・プログラムであり、前記ラベルのログを作成および記憶するステップは、活動的な表示要素タイトルをロ

グファイルに書込む請求項20記載のコンピュータ使用監視方法。

22. 前記監査するステップは、表示要素の内容を監視して、予め定められた基準を満足させる表示要素内容を識別し、

前記作成および記憶するステップは、識別された表示要素の内容をログファイルに書込む請求項19記載のコンピュータ使用監視方法。

23. 前記表示要素は編集ボックスであり、前記予め定められた基準は予め定められたシンタクスである請求項22記載のコンピュータ使用メーター。

24. 前記シンタクスは、URLシンタクスである請求項23記載のコンピュータ使用メーター。

25. さらに、オペレーティング・システム・メッセージを傍受し、オペレーティング・システム・メッセージモジュールに応答する予め定められたタイプのメッセージの受信を示すステップを含んでいる請求項23記載のコンピュータ使用メーター。

【発明の詳細な説明】

コンピュータ使用メーターおよび解析装置

発明の背景

1. 発明の分野

本発明は、コンピュータの使用状態を監視するシステムに関し、特にパーソナルコンピュータで予め選択された動作を収集し、記録し、解析し、使用状態の傾向を報告するシステムに関する。

2. 関連技術の説明

パーソナルコンピュータの人気は、この10年の間に爆発的に高まった。パーソナルコンピュータの利用人口は、使用されるパーソナルコンピュータ数やその使用方法と共に年々増加している。この急速な拡大の結果、コンピュータ、コンピュータ関連サービス、コンピュータソフトウェア、コンピュータ周辺装置、および電子情報ならびに情報サービスに使われた金額は、天文学的に増大している。わずか数年のあいだに、コンピュサーブ(CompuServe)、Prodigy、およびアメリカ・オン・ライン(America On-Line)のようなオン・ラインサービスが仮想上の不可解な言葉から周知の言葉になった。子供たちは自転車に乗ることができる前に、“ネット”をサーフすることを学ぶ。これまで、構内または広域ベースでコンピュータの使用度を測定するための効率的で信頼性の高いメカニズムがなかった。

任意のコンピュータ関連の製品あるいはサービスを販売している、または任意の電子フォーマットで任意の市場取引活動を行っている組織体の間において、コンピュータ関連のリソースの使用状態や電子情報の普及状況を測ることが強く求められている。テレビ市場を評価するためにテレビ広告主が視聴率や視聴者デモグラフィに頼るのと全く同様に、“電子”広告主および売り手、コンピュータ関連製品およびサービスの製作者はコンピュータの使用状態および“オン・ライン視聴率”に関する情報を評価することを必要としている。

発明の概要

本発明の目的は、パーソナルコンピュータのソフトウェアの使用状態に関する

信頼性の高い情報の収集を容易にすることである。

本発明の別の目的は、商業的オン・ラインサービスの高い信頼性のマルチ・メディア視聴統計値を収集し、かつインターネットのワールド・ワイド・ウェブ(World Wide Web)を含む“情報スーパーハイウェイ”へのアクセスを容易にすることである。

本発明のさらに別の目的は、それに限定されるものではないがソフトウェア製造業者、商業オン・ラインサービスのプロバイダ、コンピュータ・ハードウェア製造業者、およびオン・ライン販売者を含む多数の異なる産業部門にとって有効な報告書を作成するためにパーソナルコンピュータを使用している世帯のパネルの設立を容易にすることである。

本発明によると、オペレーティング・システム・メッセージを受けて、監視するシステムが提供されることができる。このようなメッセージは、目標を定められた種々のアプリケーションへの指令でもよいし、或はオペレーティング・システムのオーバーヘッド・メッセージであってもよい。このようなメッセージは、マイクロソフト(Microsoft Windows)オペレーティング環境のようなオペレーティング・システムソフトウェアによって内部で生成されてもよい。本発明によるシステムは、膨大なメッセージアレイをフィルタし、あるアプリケーションから別のアプリケーションへの集中的な(in focus)変化を示すメッセージのような特定のメッセージだけを捕捉することができる。これらの集中的な変化は、アプリケーション始動、アプリケーションの終了、あるアプリケーションから別のアプリケーションへのリソースの切替え、アプリケーションの最小化、またはアプリケーションの復元を含んでもよく、またこれらに限定されない。

本発明によると、オペレーティングシステム・メッセージを受けることが可能であり、適切なメッセージをその他の関連した、または有効な情報と共に、ログファイルに記録することができる。このような関連のある、または有効な情報は、日付スタンプ、時刻スタンプや、始動、終了、スイッチ、最小化、復元のようなメッセージタイプ、世帯ID番号、世帯内の個人ユーザーの識別、アプリケーションの実行可能なプログラムファイル名とファイル寸法の識別、アプリケーション

ンのウインドウタイトル、およびそのアプリケーションの“インスタンス”へのハンドルを含んでいる。世帯識別番号は、世帯の“パネル”内のパーソナルコンピュータを特有に識別する番号であってよく、各パーソナルコンピュータがローカル・測定システムを使用することによってデータをシステムに提供している。

本発明によるシステムは、複数のコンピュータおよびコンピュータユーザーと共同して使用できる点が有効である。このシステムと結び付けられたコンピュータおよびコンピュータユーザーは、はるかに広範囲のユーザーを表すように意図されてもよい。これは、限定された世帯数に基づいてテレビジョン視聴率を設定するために使用されるテレビジョン視聴情報の収集に類似している。限定された世帯数は、全体的なコンピュータの使用または“視聴”を表すものと考えられる。

本発明によると、パーソナルコンピュータ中に設置されたメーターアプリケーションは、任意の所定のアプリケーションの一番上のウインドウに対する事象をログファイルに記録することができる。アプリケーションの子ウインドウに固有の事象は、必ずしもログファイルに書込まれなくてよい。ある特定のアプリケーションに対しては、このような子ウインドウに対する追加的な詳細な事象のログファイル書込みが発生するであろう。あるアプリケーションがさらに詳細なログファイル書込みの目標とされた場合、子ウインドウの生成を示すメッセージがログファイルに記録されるであろう。ログファイル中の項目は、少なくとも日付、時刻、世帯ID番号、コンピュータを使用している世帯内の個人、親アプリケーションのインスタンスへのハンドル、親アプリケーションの現在のウインドウタイトル、および子ウインドウタイトルを含んでいることが有効である。

さらに本発明の目的は、ある特定の外部通信を監視して、ログファイルに記録することである。ローカル・メーターアプリケーションは、モデムのような通信ポートに送られた文字のストリングを監視する。システムはある予め定められた文字ストリングを監視して、このようなストリングの発生時にある情報をログファイルに書込むように設定されてもよい。例えば、システムがストリング“http:”を検出した場合、このシステムは、次に続くものがインターネットのワールド・ワイド・ウェブのハイパーテキスト・プロトコルサイトに対するユニ

バーサル・リソース・ロケータ (URL) の残りのものであることを認識する。

ローカル・メーターアプリケーションがURLを識別した場合、それは全URLを受けてログファイルに書込む。この状況において、ログ項目は、少なくとも日付、時刻、世帯ID番号、その世帯内の個人ユーザー、親アプリケーションのインスタンスへのハンドル、親アプリケーションの現在のウインドウ・タイトル、およびユニバーサル・リソース・ロケータ (URL) を含んでいてもよい。

本発明によると、アプリケーションはまた特別のログを作成し、または特別の事象をログファイルに書込んでもよい。これらの特別のログ/事象は、予め選択されたアプリケーション或はアプリケーションの、オンライン・サービスあるいはインターネットブラウザのリクエストのようなクラスに焦点を合わせてもよい。パーソナルコンピュータの焦点となる周期的な監査をトリガーするために、タイマーが使用可能である点が有効である。周期的な監査は、例えば1/2秒ごとに、または適切な別のインターバルで行われてもよい。このインターバルは、焦点となるものの移行をミスする危険を冒すという犠牲を払って処理リソースを節約するためにもっと長い期間であってもよい。

本発明の1つの特徴によると、周期的な監査は、予め選択されたアプリケーションが実行しているか否かを決定するために開いているウインドウの全てに対してオペレーティングシステムにポーリングしてもよい。このような予め選択されたアプリケーションは、アメリカ・オンライン (America On-line)、Prodigy、マイクロソフトネットワーク (Microsoft Network)、はコンピュサーブ (Compu-serve) のようなオン・ラインサービス・アプリケーションを含んでいてもよい。このようなアプリケーションが実行されている場合、メーターアプリケーションは、アプリケーションのタイトル・バーとこのようなアプリケーションの中の一番上のウインドウとのテキスト内容をログファイルに書込んでもよい。アプリケーションのタイトル・バーまたは一番上のウインドウのテキスト内容が前の監査から変化した場合にだけ、システムはタイトル・バーをログファイルに書込むことが有効である。さらに、各監査は編集ボックスのために開いているウインドウを監視してもよい。開いているウインドウ中に編集ボックスを見出たと、シス

テムは、それがURLと一致しているか否かを決定するために編集ボックスの内容のシンタクスを検査する。一致している場合、URLは事象ログまたは特別の

ログに書込まれることができる。

本発明によると、メーターアプリケーションは、コンピュータ上にメーターアプリケーションをインストールするための機構、データ記録のためのデータ圧縮および暗号化システム、ログ転送機構、自己更新ソフトウェア特徴、およびユーザーを含むその他多数の“ハウスキーピング”特徴を有していてもよい。

データ圧縮および暗号化システムは、事象ログの記憶に割当てられなければならないメモリリソースを最小にするために設けられていることが有効であり、またそこに含まれている情報のセキュリティを高めるために事象ログを暗号化してもよい。

データ転送システムは、ローカル・パーソナルコンピュータ使用ログを中央処理システムに転送するために設けられることができる。中央処理システムは、多数のローカル・パーソナルコンピュータ使用ログを取り入れ、ログ情報を有効な情報に変換し、情報を評価して、コンピュータ使用状態の種々の報告書や解析結果を作成してもよい。この転送は、自動化され、ユーザーにより開始された、或は中央局により開始された電子転送、或はディスクのような磁気記憶媒体への局所的ダウンロード、および中央処理位置へのディスクの転送を含む多数の異なる機構の任意のもので行われてもよい。

コンピュータ使用メーターおよびその支援ソフトウェアは、時々システム更新を経験する可能性がある。これらの更新は、ソフトウェアに特徴を付加して、どのようなシステムバグでも修正するように意図される。各パネリストは、前の月のログファイルに書かれた活動を収集することを目的として、月に1度が有効な同定したサイクルで連絡を取ってもよい。このプロセスは、パネリストに郵送された、或はモデムを介して電送されたディスクにより行われてもよい。どのような媒体でも転送されるデータ転送プログラムは、最初に任意の顕著なソフトウェア・アップグレードを調べることができる。あるものがスケジュールされている場合には、ソフトウェアがパネリストのコンピュータに自動的に転送され

る。

システムは、アプリケーションのタイプであるソフトウェアの特定のクラスの
使用後などのある環境にかかわるアンケートを含んでもよいし、或は事象ログま

たは別のファイルに記憶されていてもよい。所望の情報を入力するようにユーザー
が周期的にプロンプトされてもよい。データ転送システムは、回答をアップロー
ドし、また追加された質問またはトリガーをダウンロードするために使用されて
もよい。

本発明によるシステムの利点の1つは、事象ログにおけるプロセッサ注目度の
変化を記録することである。ソフトウェアの販売者は、ユーザーの彼等の製品に
対する反応についての情報を強く希望している。もしこれを行うとすれば、典型
的にペーパーアンケートまたは電話を通してのインタビューにより“使用”情報
が収集される。このような状態では、回答者は対象となる彼等自身の製品の使用
を思い出すように求められる。このテクニックは、人間の記憶力に固有の限界と
不正確さ、個々のコンピュータユーザーがこのような情報を提供するために費や
すことをいとわない時間量の限界、およびアンケートに返答する個人がコンピュ
ータシステムを使用する世帯のメンバーの1人だけであるかもしれず、関連のあ
る情報の全てを有していない可能性があることを含む重大な欠陥を示す。

本発明によるシステムは上述の欠点を克服する。最初の設置プロセスの後、シ
ステムは完全に受動的になってもよい。すなわち、コンピュータユーザーは、シ
ステムを効率的に動作させるための付加的なアクションを取る必要はない。任意
のソフトウェア製品またはアプリケーションプログラムを使用することにより、
システムにより記録されたオペレーティングシステム環境中の事象メッセージが
自動的にトリガーされる。この自動方式により、コンピュータユーザーとの後続
的な対話よりはるかに多くの情報がコンピュータによって収集されることができ
る。例えば、ある事象の日付および時刻に関する情報は、コンピュータの内部ク
ロックとカレンダーを使用して容易に獲得されてもよく、ここにおいてこのよう
な情報は、後の個人的な報告の間にユーザーによって通常思い出されないもので
ある。事象ログの構造は、典型的に有効な情報に非常に富んでおり、少なくとも

ソフトウェア・タイトルによるソフトウェア使用分類や、ソフトウェアのサブカテゴリ（例えば、スプレッドシート、スクリーンセ이버、通信ソフトウェア、個人情報管理、ワードプロセッサ等）の分類、または例えば子供の有無、収入、家の間取り等の世帯デモグラフィによる分類を可能にする。本発明によるシステム

はまた、分単位による合計使用時間、すなわち分単位による累積集中時間、使用頻度すなわち所定の時間フレーム中のアクセス数、およびコンピュータ使用のシェアによってソフトウェアの使用量を測定することができる。

有効な付加的特徴によると、システムはある特定のアプリケーションをログファイルに詳細に記録することを可能にする。商業的なオン・ラインサービス業界は非常に競争的であり、またマイクロソフト社の参入により、その競争率が高まるであろう。現在、コンピュサーブ、Prodigyおよびアメリカ・オンラインという大手3社のプロバイダが、それぞれ約2百万人の加入者を有している。これらの組織体にとって唯一最大の問題は、加入者の自然減を減らし、かつ任意の個人が定期利用契約を継続する期間を長くすることである。実際、加入者の減少は顧客の満足度の尺度であり、逆の立場から言えば、それはオンライン・サービスの収入傾向と関係している。このような減少を減らすことは、加入者をより長期間にわたって確保し、かつ収入を増加するということを意味する。

本発明によるシステムは、商業的なオン・ライン・サービスのプロバイダやユーザーアプリケーションのために子ウインドウ情報を収集することができる点が有効である。これらのアプリケーションの子ウインドウのウインドウ・タイトルは、一般にその瞬間における活動の役に立つ記述を有している。例えば、加入者がそのサービス用のメールシステムを使用している場合、このウインドウ・タイトルがそのように示す。本発明によるシステムは、ログファイルにこれらのタイトルを記録する。

例示すると、電子メールメッセージを書込むためのウインドウのウインドウタイトルは、コンピュサーブでは“メールを書きなさい”であり、Prodigyでは“書込め”であり、またアメリカ・オンラインでは“メールを作成せよ”である。

この情報の収集と解析は、競争的なサービスの種々の特徴に費やされた時間の分布、それぞれの特徴のいずれが多数のサービスのユーザーによって好まれたかの識別、および種々のサービスのいずれの特徴の人気の高いかの識別、およびこれらの特徴への注目度が加入契約期間の長さに関連して変化する状態を含み、それらにだけ限定されないが、多くの点でオン・ラインのサービスプロバイダにとって貴重である。ログに記録された情報は、顧客についての直接的なフィードバック

をオン・ラインサービスのプロバイダに提供し、かつサービスを改良すべきエリアを指摘することができるので、プロバイダにとって貴重である。本発明によるシステムはまた、電子マガジンや新聞のような商業的なオン・ラインサービスのオン・ライン内容エリア内のトラフィックを測定することができる。出版業者がオン・ラインメディアに進出すると、メディア・トラフィック統計値が重要になる。それは重要なデータをメディア立案者に提供する。さらに、本発明の有効な特徴は、通信ポートまたはモデムのトラフィックを傍受してログファイルへ記録する。商業的オン・ラインサービスに関する活動を追跡する延長として、本発明によるシステムは、それがまたインターネットのワールド・ワイド・ウェブのような他の通信チャンネル上のトラフィックを測定した場合には、オン・ライン活動のフル・ピクチャーを作成することができる。ウェブ上のインターネット・サイトは、ユニバーサル・リソース・ロケータスキムによってアドレス可能である。

オン・ラインの販売者は、ウェブ・トラフィックの特徴を理解し、かつ異なるサイトでユーザーが費やす時間を把握しようとする。これらのトラフィック統計値は、コマーシャル時間の販売および価格決定の基礎としてテレビ視聴率を使用するのと同様に、メディア計画の基本データとなる。

付加的な有効な特徴によると、このシステムは、自動化されたファイル管理機能を含んでいる。これらの機能は、システムがホストコンピュータの効率的な動作を妨害することを阻止するために必要とされる。事象ログファイルは、非常に大きくなることができる。ログを可能な限り小さくしておくことが重要かもしれない。事象ログの大きさを減少するために、データ圧縮技術を使用してもよい。さらに本発明によるシステムは、可能な限り受動的なプロファイルを持続しなく

てはならない。したがって、自動化された設置およびデータ転送プログラムは、ユーザーのコンピュータ使用による妨害を減少させて、任意の特定のユーザーに対する影響を最小限にとどめる。

画面の簡単な説明

図1は、本発明のフロー図である。

図2は、本発明の1実施形態を示す。

図3は、メッセージおよび事象の転送を示す。

図4は、メッセージへの応答を示す。

図5は、監査ベースのサブシステムを示す。

好ましい実施形態の詳細な説明

本発明の1実施形態によると、パーソナル・コンピュータ・リソースの使用に関する情報を収集し、処理して転送するシステムが提供される。図1は、本発明による1実施形態のフロー図を示す。コンピュータ使用メーター1は、パネリストまたはユーザーのグループ10によって所有され、および、または動作されるパーソナル・コンピュータの上に設置されてもよい。パネリストは有効に特定の世帯のメンバーを指し、また1人以上の個人から構成されてもよい。コンピュータ使用メーターは、有効に事象ログファイル11を生成する。機構2は、中央処理ステーションに事象ログファイルを転送するために設けられている。この転送は、フロッピーディスクのような可搬性の媒体への転送によって、または電話リンクのような通信チャネルを介して、或は電子メールによって行われてもよい。転送は、時間、ログファイルに書込まれた事象の数、ログファイルの大きさ、使用された、または利用可能なリソース、或はそれらの任意の組合わせのような任意の予め定められた基準によって行われてもよいし、或はトリガーされてもよい。中央処理ステーションは、複数の別個のコンピュータ使用メーター12からのログファイルを蓄積する。位置3における中央処理ステーションは、複数の事象ログファイルからの情報を有しているデータベース13をロードする。中央処理ステーションはマイクロプロセッサベースのコンピュータであってもよいし、またコンピュータ使用データベース13を管理し、カスタム化されたデータ辞書14を作成する

ために種々の市販の、および、またはユーザー独自に作成したデータベース管理システム4を使用してもよい。カスタム化されたデータ辞書は、事象ログファイルによって供給された生データを解釈するために設けられている。さらに、データベース管理システム4は、有効な情報を抽出し、予備処理および／または蓄積された事象ログファイルの解析を行ってもよい。このシステムはまた位置15において使用データを識別する。カスタム化された辞書によって認識されない、ログファイルに書込まれている任意の事象は、例外として認識され、その後の手動式の識別のために記憶される。この段階でのユーザーまたは手動式の介入は、それ

以上の識別を可能にし、またカスタム化された辞書14は、類似した事象の後続的な発生がカスタム化された辞書14によって自動的に識別されるように更新されることができる。カスタム化された辞書または手動式の介入15のいずれかにより識別されたログ事象は全て、位置5において情報の生データベースを作成するために使用される。このデータベースは、異なるデータベース管理システムによって組織化されてもよい。データベースは、NPDグループ社から販売されているNPD／POWERVIEWデータベース16の形態のデータベースであることが意図されている。

位置6において、パワービュー(Powerview)データベース管理システムは、後続する解析7のためにデータベースにおいて報告または予備処理情報を生成してもよい。システムは、保持されたデータベース要素から生じた情報を示す報告を生成してもよい。データは組織化され、事実上任意の所望の方式および構成で報告されてもよい。種々の市販のデータベース管理システムが長所と短所を有しているとすれば、ハード・コピー報告17を生成するために、或はその場限りの解析または報告生成18のために使用可能なサブ・データベースを作成するために、データが1以上のデータベース管理システムによって処理されてもよい。

図2は本発明によるコンピュータ使用メーターを示し、ウィンドウズ(Windows)環境で動作しているIBM適合パーソナル・コンピュータにインストールされた情報およびデータ流を表している。ウィンドウズ環境は、種々のモジュールによって使用されるメッセージを内部で生成し、コンピュータのオペレーションを

管理し、そのリソースを割当てる。ほとんどのアプリケーション・プログラム作成には、オペレーティング・システムによって処理される内部オーバーヘッドによる処理が不要である。ウインドウ環境は、内部駆動装置を使用することによって膨大なオーバーヘッド機能アレイを処理する。内部駆動装置はウインドウ・キーボード駆動装置20およびウインドウ・マウス駆動装置21を含んでいてもよい。これらの駆動装置は、オーバーヘッドがマウスポインタを操作し、マウスボタンをクリックし、またキーボード上で情報を入力するのを管理する。マウス事象やキーボード事象のようなユーザ・インタフェース事象は、ウインドウ・ユーザ・モジュール22に転送される。

図2に示されているように、コンピュータ使用メーターの主要動作モジュール23はRITAとして示されされており、それ自身のウインドウ内で動作する。ウインドウ・ユーザ・モジュール22は、WM_CREATE、WM_SYSCOMMAND、WM_COMMAND、WM_QUERYENDSESSION、およびWM_DESTROYのようなアプリケーション・特定メッセージを生成する。これらのメッセージは特定の主ウインドウ・アプリケーション・モジュールだけに使用されるように意図されている。RITAモジュール23は、RITAアプリケーション・主ウインドウ23を呼出す命令のためにこれらのメッセージを監視する。HOOKS DLLモジュール24は、呼出された後、RITA主ウインドウ・モジュール23にメッセージを与えるように動作する。パーソナル・コンピュータの動作中、ウインドウ・ユーザ・モジュール22は、ウインドウ・コール・バックまたは“CBT”事象を生成する。ある特定の事象はHOOKS DLLモジュールにより傍受され、RITA主モジュール23に転送される。RITA主ウインドウは、このようなメッセージを受取ると、ある特定のメッセージをRITAログファイル記録サブシステム24に送る。さらに、RITA主ウインドウ23は、RITA INIファイル・サブシステム25にプログラム実行時間パラメータを転送する。このRITA INIファイル・サブシステム25は、パネリスト名を収集するためにパネリスト情報ダイアログ・ボックス26と通信する。このパネリスト情報ダイアログ・ボックス26はまた、RITA主ウインドウ

23に活動的なユーザー名を転送する。活動的なユーザー名は、ログファイル記録動作に関連して使用される。

図3は、ウインドウCBT事象およびウインドウ・ユーザー定義メッセージの転送を示す。ウインドウ・ユーザー・モジュール22がHCBT__ACTIVATEメッセージを生成すると、このようなメッセージはHOOKS DLLモジュールによって認識され登録される。HCBT__ACTIVATEは、現在活動的なウインドウと、始動させられようとしているウインドウの識別を表す。HOOKS DLLモジュールは、HCBT__ACTIVATEを受取ると、WH__HCBT__ACTIVATEをメッセージを送って、始動させられているウインドウのRITAによるログファイルへの書き込み用のハンドルを示す。このハ

ンドルは、マイクロソフト・ウインドウズの活動的なプロセスを固有に識別した整数である。ウインドウ・ユーザー・モジュール22から新たに作られたウインドウのハンドルを示すHCBT__CREATEWNDメッセージを傍受すると、HOOKS DLLモジュール24は、ログファイルに記録するためにWH__HCBT__CREATEWNDをRITAに送る。破壊されようとしているウインドウのハンドルを示すウインドウ・ユーザー・モジュール22からのHCBT__DESTROYWNDメッセージを傍受すると、HOOKS DLLモジュール24は、ログファイルに記録するためにWH__HCBT__DESTROYWNDメッセージをRITA主ウインドウ23に送る。最小化または最大化されようとしているウインドウのハンドルを示すウインドウ・ユーザー・モジュール22からのHCBT__CBT__MINMAXメッセージを傍受すると、HOOKS DLLモジュール24は、WH__HCBT__CBTMINMAXメッセージをRITA主ウインドウ23に送る。HCBT__CBTMINMAXメッセージは、それぞれがウインドウが最小化されている、最大化されている、復元されているかどうかを示す動作コードであるいくつかの形態を取ることができる。受信された動作コードに応じて、HOOKS DLLモジュール24は、SW__HIDE、SW__SHOWMINIMIZED、SW__MINIMIZE、SW__RESTORE、SW__MAXIMIZE、SW__NORMAL、またはSW__SHOWを含むいくつ

かのメッセージの1つをログファイルに書込むためにR I T Aに送る。

図4は、ウインドウ・ユーザー・モジュール22によって生成されたウインドウズ・アプリケーション・メッセージに対するR I T A主ウインドウ23の応答を示す。ブロック27は、WM__CREATEメッセージに対するR I T A応答を示す。WM__CREATEメッセージは、アプリケーションがスタートしていることを示す。応答がパネリストIDメッセージをプロンプトし（これが最初ならば、アプリケーションが実行される）、METER動作コード項目をログファイルに書込み、PANEL動作コード項目をログファイルに書込み、START動作コード項目をログファイルに書込み、1以上のRUNNGタスク項目をログファイルに書込む。パネリストIDに対するプロンプトは、パネリストが予め定められた7桁の番号により独自の識別を可能にする。以下に説明するように、ログファイル

に書込まれた各事象にはログ項目の構成が必要である。各項目は、ログファイルに記録されている事象のタイプを示す動作コードを含む。RUNNGタスク項目は、コンピュータ使用メーターが主R I T Aモジュールにより呼出されたときに、既に動作しているどのウインドウズ・アプリケーションに対してでもログファイルに書込まれる。ブロック28は、WM__SYSCOMMANDメッセージに対するR I T A応答を示す。WM__SYSCOMMANDメッセージは、ユーザーがウインドウズ・デスクトップからHT Iアイコンを付勢させたことを示す。応答によって、ユーザー・ダイアログを変更し、PANEL動作コード項目をログファイルに書込む。ユーザー・ダイアログの変更は、次のログファイルに書込まれたレコードに記憶されたユーザ名に影響を与える。ブロック29は、WM__QUERYENDSESSIONメッセージへのR I T A応答を示す。WM__QUERYENDSESSIONメッセージにより、ウインドウズはシャットダウンしているが、それがきちんとそれ自身を閉じるように、最初にR I T Aに制御を渡すことを示す。応答によって、STOPM動作コード項目をログファイルに書込み、ログをクリアする。ブロック30は、ユーザー・モジュールによって生成されたWM__DESTROYメッセージに対するR I T A応答を示す。WM__DE

STROYメッセージは、ユーザーが明確にRITAを閉じたことを示す。この応答によって、STOPM動作コード項目をログファイルに書込み、ログをクリアする。ログ・クリア動作は、メモリに依然として保持されている任意のレコーをログファイルに書込むことから成る。

ログファイルは、データを記憶するために固定したコラムフォーマットを使用してもよい。最初のコラムは、ポストプロセッサの文解析のために使用されることのできるロギング・シーケンス番号を含んでもよい。ログファイルはまた、日付スタンプおよび時刻スタンプが各レコードに与えられるコラムを含んでいてもよい。次のコラムは、以下のような動作コードを含んでいてもよい：

- RUNNG これは既に実行しているタスクを示す
- PANEL パネリスト名および識別が記録データ部分に配置される
- METER アプリケーション・ログおよびバージョン情報

- START メーターをスタートする
- ACTVT 一番上のウインドウ・タスクが始動させられたことの記録
- TSTRT 一番上のウインドウ・タスクがスタートしたことの記録
- TSTOP 一番上のウインドウ・タスクがストップしたことの記録
- MINIM 一番上のウインドウが最小化されたことの記録
- RESTO 一番上のウインドウがそのアイコン状態から復元または最大化された状態からその元の状態に復元されたことの記録
- STOPM メーターをストップする
- INTRV レコード・データをインタビューする

以下にログ項目の一例を示す。

00001	05/25/95	10:40:27	METER	1234561 0000	[D=02.00-02]
00002	05/25/95	10:40:27	PANEL	1234561 0000	[D=John Doe]
00003	05/25/95	10:40:27	START	1234561 0000	[D=ini StartTask=1 EndTask=1 Minimize=2 Maximize=1 Activate=1 Restore=1 Running=1]
00004	05/25/95	10:40:27	RUNNG	1234561 2a96	[D=C:\DOS\MOUSE\POINTS REXS] [T=Pointer Options] [S=10432]
00005	05/25/95	10:40:27	RUNNG	1234561 201e	[D=C:\WINDOWS\NETDDE. XS] [T=NetDDE] [S=\$2432]
00006	05/25/95	10:40:27	RUNNG	1234561 1f6e	[D=C:\WINDOWS\SYSTEM\ DDEML.DLL] [S=39424]
00007	05/25/95	10:40:27	RUNNG	1234561 0736	[D=C:\WINDOWS\SYSTEM\ USER.EXE] [S=264096]
00009	05/25/95	10:40:27	RUNNG	1234561 37de	[D=C:\HTTP\HTTP.EXE] [T=HTTP] [S=59656]
000010	05/25/95	10:40:27	MINIM	1234561 37de	[D=C:\HTTP\HTTP.EXE]
000011	05/25/95	10:40:28	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH. EXE]
000014	05/25/95	10:40:29	TSTRT	1234561 357e	[D=C:\APPWIN\OMGUI\ OMGUI.EXE] [T=OpenMail user 'pinaley' on server 'ny'] [S=443360]
000015	05/25/95	10:40:33	TSTRT	1234561 36d6	[D=C:\WINDOWS\UALALLO. EXE] [S=3776]
000016	05/25/95	10:40:33	TSTRT	1234561 08ce	[D=C:\WINDOWS\SYSTEM\ HSASRV.EXE] [T=Windows Sockets Asynchronous Request Server] [S=6505]
000017	05/25/95	10:40:34	TSTOP	1234561 357e	[D=C:\APPWIN\OMGUI\OMC UI.EXE]
000018	05/25/95	10:40:34	TSTRT	1234561 357e	[D=C:\APPWIN\OMGUI\OMC UI.EXE]

000019	05/25/95	10:40:34	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000022	05/25/95	10:40:36	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000024	05/25/95	10:40:36	TSTOP	1234561 1fe6	[D=C:\WINDOWS\SYSTEM\DDDEML.DLL]
000025	05/25/95	10:40:36	TSTOP	1234561 1fe6	[D=C:\WINDOWS\SYSTEM\DDDEML.DLL]
000026	05/25/95	10:40:40	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000027	05/25/95	10:40:40	TSTRT	1234561 2fe6	[D=C:\WINDOWS\CALC.EXE] [T=Calculator] [S=43072]
000028	05/25/95	10:40:41	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000029	05/25/95	10:40:43	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000030	05/25/95	10:40:43	TSTRT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE] [T=Cardfile - (Untitled)] [S=93184]
000031	05/25/95	10:40:44	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000032	05/25/95	10:40:46	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000033	05/25/95	10:40:46	TSTRT	1234561 2b16	[D=C:\WINDOWS\notepad.EXE] [T=Notepad - (Untitled)] [S=32736]
000034	05/25/95	10:40:46	ACTVT	1234561 2b16	[D=C:\WINDOWS\notepad.EXE]
000035	05/25/95	10:40:51	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000036	05/25/95	10:40:57	ACTVT	1234561 2fe6	[D=C:\WINDOWS\CALC.EXE]
000037	05/25/95	10:40:58	MINIM	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000038	05/25/95	10:40:58	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000039	05/25/95	10:41:00	ACTVT	1234561 2b16	[D=C:\WINDOWS\notepad.EXE]
000040	05/25/95	10:41:02	TSTOP	1234561 2b16	[D=C:\WINDOWS\notepad.EXE]

000041	05/25/95	10:41:02	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000042	05/25/95	10:41:04	ACTVT	1234561 2fe5	[D=C:\WINDOWS\CALC.EXE]
000043	05/25/95	10:41:05	RESTO	1234561 2fe6	[D=C:\WINDOWS\CALC.EXE]
000044	05/25/95	10:41:06	TSTOP	1234561 2f36	[D=C:\WINDOWS\CALC.EXE]
000045	05/25/95	10:41:06	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000046	05/25/95	10:41:08	TSTOP	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000047	05/25/95	10:41:08	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000048	05/25/95	10:41:16	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000049	05/25/95	10:41:19	STOPM	1234561 0000	[D=Windows Shutdown]

ログ項目表に示されているように、各項目は、シーケンス番号、日付スタンプ、時刻スタンプ、動作コードまたは事象タイプと、データフィールドを含む。データフィールドに含まれている情報は、事象タイプによって指図される。示されている例において、次のフィールドは、パネリストまたはユーザー識別、この場合は、存在するならばアプリケーションのインスタンスへのハンドルを含むフィールドにより後続される“1 2 3 4 5 6 1”を含む。ログレコード・シーケンス番号00001は、データフィールド中にアプリケーション、ロゴおよびバージョン情報を記録するメーター動作コード項目を有している。シーケンス番号00002を有するログ項目では、PANEL動作コードがパネリストの名前を記憶するように与えられ、それはまた別の識別情報を記憶してもよい。この例において、記録された名前はジョン・ドウ(John Doe)である。アプリケーションが始動させられると、コンフィギュレーション情報をデータフィールドに記録するSTART動作コードのログ項目が形成される。有効な実施形態によると、コンピュータ使用メーターは、始動の後に自動的に最小化される。その他の適切な情報が種々の事象タイプのログ項目のデータ部分に含まれていてもよい。データフィールドは、ラベルによって識別される異なる情報を含んでいてもよい。示された例において、ラベル“S”はアプリケーションのファイル寸法を識別する。ラベル“T”は、アプリケーションのウィンドウズ・タイトルを識別する。ラベル“D”は、

典型的にアプリケーションの全経路である、種々のデータを識別する。その他のラベルおよび情報もまたログファイルに書込まれることが可能である。

本発明の別の実施形態によると、使用メーターは、同じログファイルに、或は補助ログファイルのいずれかに付加的な事象を記録してもよい。付加的な事象は、周期的な監査に基づいてログファイルに書込まれることができる。周期的な監査は、タイマーによってトリガーされてもよい。そのタイマーはソフトウェアで実行されると有効であり、またそれ自身のウインドウの中で、或はシステムレベルで動作してもよい。監査は、その他のトリガー周期が選択されてもよいが、1/2秒ごとにトリガーされると有効である。使用メーターは、オン・ラインのプログラム活動に対してコンピュータ使用を周期的に監査してもよい。メーターは、予め定められた或いは予め選択されたコンピュータ・アプリケーション、またはモデムアクセスのような予め定められたリソースに頼るアプリケーションに対してコンピュータを監査するように設定されてもよい。予め選択されたコンピュータ・アプリケーションは、アメリカ・オンライン、コンピュサーブ、Prodigyまたはマイクロソフト・ネットワークによって提供される周知のオンラインサービス・アクセスと、インタフェース・アプリケーションであってもよい。予め選択されたアプリケーションの1つが表示されるか、或いはその代わりに始動させられていることが監査によって明らかにされた場合、アプリケーション・ウインドウと一番上のウインドウとからの情報がログファイルに書込まれる。ログファイルに書込まれた情報は、アプリケーションのタイトルバーのテキスト内容と、このようなアプリケーションの一番上のウインドウのテキスト内容であってもよい。好ましい改善によると、システムは、アプリケーションまたは一番上のウインドウのタイトルバーの内容が同じアプリケーションに対して前にログファイルに書込まれたタイトルバーと異なっている場合には、タイトルバーのテキスト内容だけをログファイルに書込む。

周期的な監査特徴の別の実施形態は、予め選択されたタイプの表示要素を周期的に監査することを含んでいる。ウインドウズ・オペレーティング・システムにおいて、それぞれ表示されたウインドウは、多数の表示要素で構成されている。この表示要素は、特に編集ボックスとボタンを含んでいる。好ましい特徴による

と、編集ボックスの内容は検査されることができる。内容が予め定められた基準と一致している場合、この内容はログファイルに書込まれる。例えば、編集ボックスの内容がURLに対するシンタクスと一致している場合には、ウィンドウがインターネット・ブラウザ・プログラムに対応していると考えられる。編集ボックスの内容をログファイルに書込むということは、インターネット上の文書のユーザーのアクセスを示す。

図5は、監査ベースの使用メーターを示す。監査ベースのサブシステムはタイマー40を含んでいる。タイマー40は、監査モジュール41をトリガーする。監査モジュールは、監査ターゲット42の内容を予め定められた基準43と比較する。予め定められた基準が満足された場合、監査モジュールは、事象ログ44において項目を作成する。ターゲットは、コンピュータ使用と活動とを示す表示または他の情報であってもよい。基準43は、予め定められたアプリケーション・プログラム、ウィンドウズ、または例えばインターネット、特にワールド・ワイド・ウェブ用のURLと一致したシンタクスのようなシンタクスの識別であってもよい。

当業者は、本発明による使用メーターが本発明の基本的な概念の範囲内において種々の方法で変更されてもよいことを理解するであろう。

【図1】

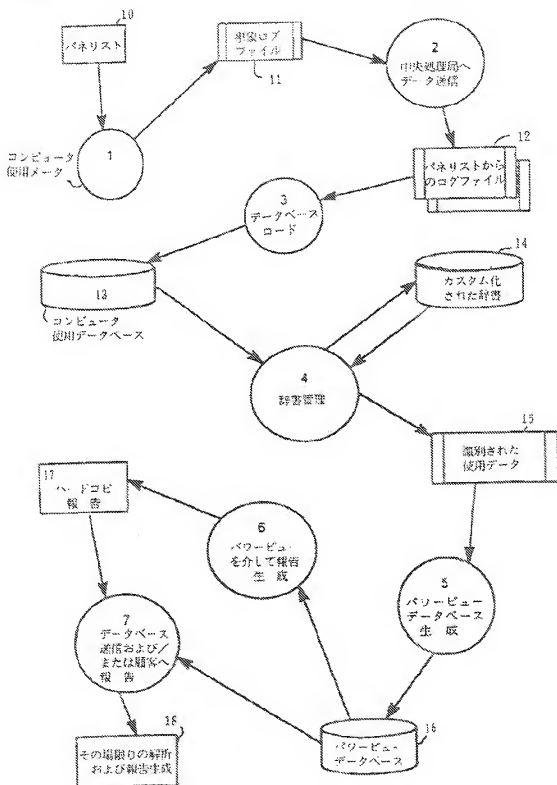


Figure 1

【図2】

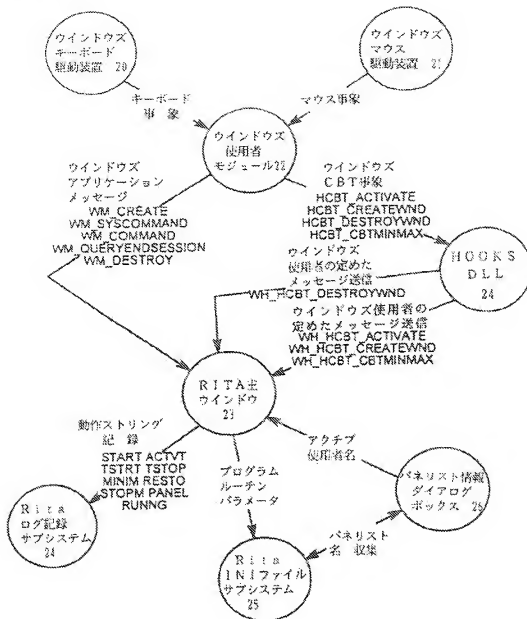


Figure 2

【図3】

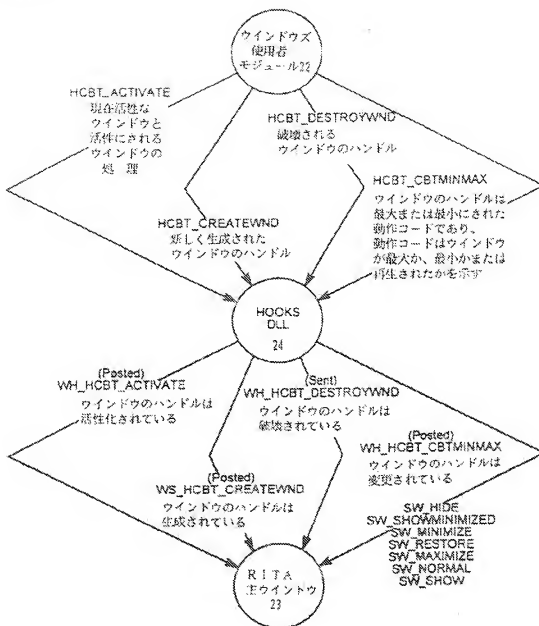


Figure 3

【図4】

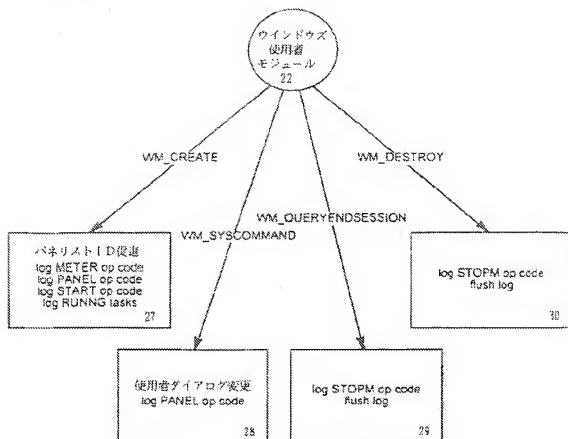


Figure 4

【図5】

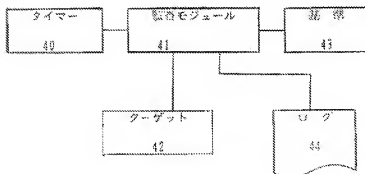


Figure 5

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/10091

A. CLASSIFICATION OF SUBJECT MATTER

IPC(Cl.) : B60G 9/02

US CL. : 364/222.2, 222.5, 940.1; 395/600

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/222.2, 222.5, 222.81, 940.1; 395/600

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 5,032,979 (HECHT ET AL.) 16 July 1991, abstract and col. 11.	1-12 and 16-18
X	US, A, 5,406,269 (BARAN) 11 April 1995, abstract and fig. 1.	1-5 and 9-14
A	US, A, 4,827,508 (SHEAR) 02 May 1989, abstract.	1-25
A, P	US, A, 5,483,658 (GRUBE ET AL.) 09 January 1996, abstract.	1-25

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of prior documents:	* Documents published after the international filing date or priority date and not in compliance with the provisions that tend to undermine the principle of novelty underlying the invention.
* "A" document defining the general state of the art which is not considered to be part of particular relevance	* "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken into account.
* "S" earlier document published on or after the international filing date	* "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combinations being obvious to a person skilled in the art.
* "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reasons (as specified)	* "G" document member of the same patent family
* "O" document referring to an oral disclosure, use, exhibition or other means	
* "P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search:

30 JULY 1996

Date of mailing of the international search report

18 SEP 1996

Name and mailing address of the ISA/US
Communication of Patents and Trademarks
Box PCT
Washington, D.C. 20533

Facsimile No. (703) 305-3220

Authorized officer

CRAIG STEVEN MILLER

Telephone No. (703) 305-3800

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, MI, MR, NF, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN

(72)発明者 ビンスレイ、 デイビッド・ビー

アメリカ合衆国、 ニューヨーク州
11021、グレート・ネック、バーストウ・
ロード・5ディール 8

(72)発明者 ボロニウィッツ、 カレン・エー

アメリカ合衆国、 ニューヨーク州
11733、イースト・セーターゲット、パッキ
ンガム・メドウ・ロード 2

(72)発明者 コステロ、 ステューブ・ジェイ

アメリカ合衆国、 ニューヨーク州
11788、ホッポージ、ジョン・ストリート
122

(72)発明者 スタンジアーニ、 ステューブ・エス

アメリカ合衆国、 ニューヨーク州
11803、ブレインビュー、ブローラル・ア
ベニュー 236

ABNORMALITY MONITORING SYSTEM

Publication number: JP11003246 (A)

Publication date: 1999-01-06

Inventor(s): KARIYA MASATOSHI -

Applicant(s): MEIDENSHA ELECTRIC MFG CO LTD *

Classification:

- International: G06F11/30; (IPC1:7); G06F11/30

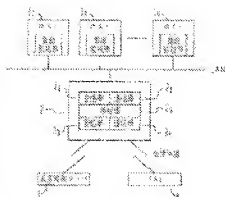
- European:

Application number: JP19970152749 19970611

Priority number(s): JP19970152749 19970611

Abstract of JP 11003246 (A)

PROBLEM TO BE SOLVED: To enable a system manager to accurately recognize the state of abnormality and to process the abnormality by using a function to estimate occurrence of the abnormality and also a function to collect and send the detailed error information based on the estimation of occurrence of the abnormality. **SOLUTION:** In an abnormality monitoring system, an abnormality processor 2 detects the abnormality of computers 11 to 1N respectively and sends the detected abnormality to the sending destination such as a system manager, etc., via a circuit. The processor 2 includes the sending parts 22 and 24 which send the information converted into the data to a LAN and the circuit, and an analysis part 25 which buffers the information transferred between the sending and receiving parts and analyzes the abnormality. Then, the part 25 collects the error information from the computers 11 to 1N and sends these information to a prescribed sending destination. Furthermore, the part 25 analyzes the queue data received from each computer to estimate the occurrence of abnormality and then collects the detailed error information from each computer to send them to the prescribed sending destination.



特開平11-3248

(43) 公開日 平成11年(1999)1月6日

(51) Int. Cl.⁵

識別記号

F I

G 0 6 F 11/30

G 0 6 F 11/30

K

審査請求 未請求 請求項の数 1 O L (全 4 頁)

(21) 出願番号 特願平9-152749

(22) 出願日 平成9年(1997)6月11日

(71) 出願人 000008105

株式会社明電舎

東京都品川区大崎2丁目1番17号

(72) 発明者 舩谷 正年

東京都品川区大崎2丁目1番17号 株式会社

明電舎内

(74) 代理人 弁理士 志賀 富士弥 (外1名)

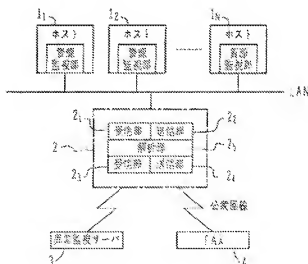
(54) 【発明の名称】 異常監視方式

(57) 【要約】

【課題】 各コンピュータがLANで接続されるコンピュータシステムに異常処理装置を接続し、この異常処理装置が各コンピュータからの異常情報をシステム管理者等に送信するのみでは、異常の分析や対応処理ができない。

【解決手段】 異常処理装置とは、LAN及び公衆回線に対するデータ変換した情報の送信部22、23と受信部21、23及び送受信情報をデータベースにバッファリングして異常を解析する解析部23を備え、解析部は、各コンピュータ11～1nからのエラー情報を収集して予め定めた異常監視サーバ3やシステム管理者のPAX4に送信する機能と、各コンピュータからのキューデータを解析して異常発生を予測し、この予測がなされたときに当該コンピュータから詳細エラー情報を収集して予め定めた送信先に送信する機能とを備える。

システム構成図



【特許請求の範囲】

【請求項1】 各コンピュータがLANで接続されるコンピュータシステムに異常処理装置を接続し、この異常処理装置が各コンピュータの異常を検出してシステム管理者等の送信先に回線を通して送信する異常監視方式において、

前記異常処理装置は、LAN及び回線に対するデータ変換した情報の送信部と受信部、及びこれら送信部と受信部による送受信情報をデータベースにバッファリングして異常を解析する解析部を備え、前記解析部は、各コンピュータからのエラー情報を収集して予め定めた前記送信先に送信する機能と、各コンピュータからのキューデータを解析して異常発生を予測し、この予測がなされたときに当該コンピュータから詳細エラー情報を収集して予め定めた送信先に送信する機能を備えたことを特徴とする異常監視方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、LAN（ローカルエリアネットワーク）で接続されるコンピュータシステムにおける異常監視方式に関する。

【0002】

【従来の技術】 プラント等の監視制御システムは、LANで接続されるコンピュータシステムを構築しており、プロセスコントローラによる現場機器の監視制御と、これらにLANで接続されるホストコンピュータによる監視管理との監視制御を可能にする。

【0003】 この監視制御システムにおいて、コンピュータの異常監視は、各コンピュータでの異常発生を検出してシステム管理者に通知する異常処理装置がLANに接続されている。

【0004】 この異常処理装置は、異常検出部と異常通知部で構成され、異常検出部では主としてコンピュータのハードウェアの異常信号からシステムのハードウェアの異常を監視し、異常通知部では専用回線又は公衆回線を利用して予め登録されている連絡先に対して音声又は視覚的に異常を通知する。

【0005】

【発明が解決しようとする課題】 従来の異常処理装置による異常監視方式は、異常発生の有無をシステム管理者に通知するのみであり、異常状況等の詳細な情報を通知する機能を持たないし、異常発生に対する処理機能を持たない。

【0006】 このため、システム管理者は、ある資源に異常が発生したことを認識できるが、どのような異常発生かを認識できないし、異常発生に対する適切な迅速な処理操作を行うのが難しい。

【0007】 本発明の目的は、異常発生時にシステム管理者が異常状況の迅速な認識及び異常処理ができる異常監視方式を提供することにある。

【0008】

【課題を解決するための手段】 本発明は、異常処理装置に異常の受動的な検出機能に加えてキューデータの能動的な収集により異常発生を予測する機能と、異常発生の際に詳細なエラー情報を収集して送信する機能とを持たせるようにしたもので、以下の方式を特徴とする。

【0009】 各コンピュータがLANで接続されるコンピュータシステムに異常処理装置を接続し、この異常処理装置が各コンピュータの異常を検出してシステム管理者等の送信先に回線を通して送信する異常監視方式において、前記異常処理装置は、LAN及び回線に対するデータ変換した情報の送信部と受信部、及びこれら送信部と受信部による送受信情報をデータベースにバッファリングして異常を解析する解析部を備え、前記解析部は、各コンピュータからのエラー情報を収集して予め定めた前記送信先に送信する機能と、各コンピュータからのキューデータを解析して異常発生を予測し、この予測がなされたときに当該コンピュータから詳細エラー情報を収集して予め定めた送信先に送信する機能を備えたことを特徴とする。

【0010】

【発明の実施の形態】 図1は、本発明の実施形態を示す異常監視システムである。ローカルホスト群になる各コンピュータ11〜18はLANで互いに接続され、このLANに異常処理装置2が接続される。

【0011】 異常処理装置2は、LANを通して各コンピュータ11〜18との通信機能を持ち、さらに、公衆回線を通して異常処理装置の上位になる異常監視サーバ3やシステム管理者のファクシミリ（FAX）に対する通信機能を持つ。

【0012】 異常処理装置2の受信部21及び送信部22は、LANを通してコンピュータ11〜18からのデータ変換機能を持って資源情報の受信及び異常発生時のエラー情報の要求出力等を行う。同様に、受信部23及び送信部24は、公衆回線で遠隔地に接続されたサーバ3等とのデータ送受信を行う。

【0013】 異常処理装置2の解析部25は、異常発生時にコンピュータ11〜18からの受信データを分析し、その結果により対応を判断し、システム内の監視対象への制御指令や公衆回線により接続された機器へのデータ送信を決める。

【0014】 このような構成になる異常処理装置2により、監視対象コンピュータから異常通知受へのデータ変換と送信にともなう、解析部25を持つことで異常状況に能動的に対応することが可能となる。

【0015】 異常処理装置2による機能関連図を図2に示す。異常通知は、一般に受信部21→解析部25→送信部24の経路で行われる。受信部23と解析部25の間のデータ授受は、データベース26を介することにより、データのバッファリングを可能にする。また、解析部2

5から送信部2へのデータ収集要求を出すことで、より詳細な情報を収集できる。

【0016】送信部2では、登録された通知先に合わせてデータ変換し、その結果を送信する。

【0017】公衆回線上に接続された異常監視サーバがある場合には、受信部2→解析部2→送信部2を経由して情報収集あるいは障害復旧の制御指令を出力する。

【0018】図3は、異常処理装置2の解析部2の処理フローを示す。同図の(a)に示すエラー情報解析処理は、エラー信号が発生したときに異常を検知し、登録先に通知する受動的処理になる。具体的には、データベース26に異常データが収集されたとき(S1)、この異常データの分析により送信先(登録先)を検出し(S2)、すべての送信先に異常データを送信する(S3～S5)。

【0019】同図の(b)に示すキューデータ解析処理は、定期的な収集情報から能動的に異常を予測すると共に、異常と判断したときには必要に応じたエラー情報要求を出力する。具体的には、コンピュータのうち、キューデータの使用情報が(S11)、一定値以上の資源を使用し(S12)、一定時間以上に資源を占有しているとき(S13)、当該コンピュータに詳細エラー情報の要求を出力し(S14)、この情報の分析により送信先の検出(S15)でデータを送信する(S16～S18)。

【0020】なお、各コンピュータの資源の使用量と占有時間は、システムの規模や負荷設定に応じて任意に設定され、この組み合わせを予め決定し、その値を変更することで監視レベルを設定可能にする。

【0021】

【発明の効果】以上のとおり、本発明によれば、異常処理装置に異常の受動的な検出機能に加えてキューデータ

の能動的な収集により異常発生を予測する機能と、異常発生の際に詳細なエラー情報を収集して送信する機能とを持たせるようにしたため、以下の効果がある。

【0022】(1)異常の能動的な予測と詳細データ収集により、異常発生時にシステム管理者が異常状況の適確な認識及び異常発生に対する適確な処理ができる。

【0023】(2)異常情報の分析により送信先を決定するため、適確な情報送信ができる。

【0024】(3)異常の予測にレベル設定可能とすることにより段階的なエラー予測が可能となり、また監視対象機器等への制御も可能となる。

【0025】(4)受信情報をデータベースにバッファリングすることにより、解析部では送信先毎のデータフォーマットを考慮することなく送信処理できる。また、送信部でデータ変換及び送信処理するため、異常通知先の変更が容易となる。

【0026】(5)異常処理装置の上位に異常処理サーバを設けることにより、より積極的に障害復旧が可能となる。また、データを蓄積することで障害発生プロセスを解析することが可能となる。

【図面の簡単な説明】

【図1】本発明の実施形態を示すシステム構成図。

【図2】実施形態における異常処理装置の機能関連図。

【図3】実施形態における解析部の処理フロー。

【符号の説明】

1…1台…コンピュータ

2…異常処理装置

21、23…受信部

22、24…送信部

25…解析部

26…データベース

3…異常監視サーバ

4…ファクシミリ

DECENTRALIZED SYSTEM OPERATION MAINTENANCE SUPPORT DEVICE AND OPERATION MAINTENANCE SUPPORTING METHOD

Publication number: JP10083382 (A)

Publication date: 1998-03-31

Inventor(s): NOZAWA YUKITERU

Applicant(s): TOSHIBA CORP.

Classification:

- International: G06F11/30; G06F15/00; G06F15/16; G06F15/177; G06F9/46; (IPC1-7): G06F11/30;
G06F15/00; G06F15/16; G06F9/46

- European:

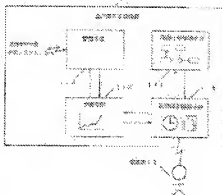
Application number: JP19960237721 19960909

Priority number(s): JP19950237721 19950909

Abstract of JP 10083382 (A)

PROBLEM TO BE SOLVED: To maintain the operation of a decentralized system effectively, economically, and deliberately by controlling a total flow for advancing operation maintenance support by an operation maintenance control means

SOLUTION: The operation maintenance control means 110 controls a series of operations for operation maintenance support by receiving a distinctive operation maintenance support request from an administrator 13 or on internal synchronism generation. Further, a work specification managing means 111 manages the correspondence relation between operation which embodies a work and the decentralized system mounted with it as specifications and provides necessary information in response to an inquiry from the operation maintenance control means 110. Further, a predicting means 112 predicts a future tendency of a constituent element of the decentralized system which is indicated by the operation maintenance control means 110 and considered to need to be maintained. Then a monitor means 113 operates as a database house for a monitor means in the operation-maintained decentralized system 10.



Data supplied from the [espacenet](http://www.espacenet.com) database — Worldwide

【特許請求の範囲】

【請求項1】 複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援装置であって、

前記分散システムの運用保守支援を開始し、さらにその後、続く運用保守支援動作を制御する運用保守制御手段と、

前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とする分散システム運用保守支援装置。

【請求項2】 複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援装置であって、

前記分散システムの運用保守支援を開始し、さらにその後、続く運用保守支援動作を制御する運用保守制御手段と、

前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、

前記分散システムの構成要素の内、運用保守制御手段により指示された構成要素の将来的な動向を予測する予測手段と、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とする分散システム運用保守支援装置。

【請求項3】 前記予測手段が、前記監視手段によって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とする請求項2に記載の分散システム運用保守支援装置。

【請求項4】 前記運用保守制御手段が、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とする請求項1乃至請求項3のいずれかに記載の分散システム運用保守支援装置。

【請求項5】 複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、

前記分散システムの運用保守支援を開始し、さらにその後、続く運用保守支援動作を制御する運用保守制御ステップと、

前記分散システムの構成要素とその分散システムに実装

される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とする分散システム運用保守支援方法。

【請求項6】 複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、

前記分散システムの運用保守支援を開始し、さらにその後、続く運用保守支援動作を制御する運用保守制御ステップと、

前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、

前記分散システムの構成要素の内、運用保守制御ステップにおいて指示された構成要素の将来的な動向を予測する予測ステップと、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とする分散システム運用保守支援方法。

【請求項7】 前記予測ステップが、前記監視ステップによって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とする請求項6に記載の分散システム運用保守支援方法。

【請求項8】 前記運用保守制御ステップが、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とする請求項5乃至請求項7のいずれかに記載の分散システム運用保守支援方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムの運用保守を支援するための分散システム運用保守支援装置および運用保守支援方法に関する。

【0002】

【従来の技術】 従来、複数の計算機およびその周辺機器をネットワークを介して構成した分散システム（以下、分散システムと総称する）については、いかにして分散システムの処理性能を上げるか、あるいは信頼性を上げるといった観点からの研究開発に重点が置かれていた。しかし、この分散システムをどのように運用保守していくべきかという点も非常に重要である。

3

【0003】ここで、上記「分散システムの運用保守」とは、「分散システムの利用者であるエンドユーザが、分散システム上に実装された業務アプリケーションを、十分有効に、かつ支障なく利用できるようにするため、分散システムの管理者が、既にサービスの提供を実施している分散システムの構成要素を適切に維持していくこと」と定義される。

【0004】たとえば、ある業務において重要な役割を担うサーバがある場合、当サーバが十分なパフォーマンスを発揮しつづけられるように、当サーバのディスクやメモリ、あるいは当サーバに接続するネットワークなどのシステムリソースを、必要に応じて強化していくといった、ハードウェアに対する作業が挙げられる。また、別の例としては、ある業務に関連したトランザクションを構成するプロセスについて、その実行をクライアント側からサーバ側へ移すといった、ソフトウェアに対する作業が挙げられる。

【0005】このような分散システムの運用保守に関する技術としては、例えば、特開平6-149737号公報に示された発明がある。この発明は、負荷分散による処理性能の向上や、危険分散による信頼性の向上、あるいはいわゆるダウンサイジングによるコストの抑制など、分散システムの利点を活かすつ、集中管理方式を導入することで、分散システムの運用保守を容易にすることを目的としている。

【0006】また、前記集中管理方式の導入にあたっては、まず、島と呼ばれる任意数の計算機およびその周辺機器からなる管理単位を設定し、この島毎にコントロールサーバと呼ばれる管理システムを割り当てる。さらに、任意数の島を一括して管理するために、マスターサーバと呼ばれる管理システムを割り当てる。

【0007】このように構成することによって、マスターサーバによる集中的／一元的な運用保守が可能となり、マスターサーバの負荷が問題になるような場合でも、ある島に特有の運用保守は、その島に割り当てられているコントロールサーバに任せることで、マスターサーバの過負荷を防ぐことを可能としている。また、このように集中管理方式を採用することによる効果として、ユーザ管理、アカウント管理、プログラム配布、ネットワーク構成管理、ネットワーク状態監視、障害対応、周辺機器の管理などを、効果的かつ容易に行うことができるとしている。

【0008】しかし、分散システムの運用保守にあたって、前記発明によっても解決されない課題が残る。すなわち、前記発明においては、分散システムを、その上に実装されている業務アプリケーションの持つ「意味」とは関係なく運用保守しているため、業務上重要と思われる管理対象と、さほど重要と思われる管理対象とが、同レベルで等しく管理されることになる。その結果、分散システムのエンドユーザが「もっとも重

4

要である」と考えている業務に関連した運用保守対象が優先して運用保守されないという問題が生じていた。また、すべての管理対象が同レベルで管理されるため、運用保守にかかるコストに無駄が生じるという問題も生じていた。

【0009】例えば、前記発明に示されているサーバの障害検知の実施例についてみると、前記発明においては、分散システムのエンドユーザがもっとも重要であると考えている業務のためのサービスを、どのサーバが請け負っているのかについて把握することができないため、エンドユーザにとって重要度の高い業務に関連したサーバが優先して運用保守されなかった。また、分散システムの管理者は、分散システムに含まれるすべてのサーバについて、一律なコストをかけて管理しなければならず、分散システムの運用保守にかかるコストに無駄が生じていた。

【0010】さらに、前記発明においては、分散システム内で発生した障害などについての運用保守に必要な情報は、それらの障害などが起こったあとに初めて分散システムの管理者によって把握されるので、運用保守が常に後手にまわってしまうという問題が生じていた。その結果、分散システムのエンドユーザは、分散システム内で発生した障害などによって、本来受けられるべきサービスが突然受けられなくなったり、あるいは非常に低い処理性能のもとでしかサービスを受けられなくなったりするなど、本来の品質を保ったサービスを享受することができず、多大な不利益を被る危険性があつた。

【0011】すなわち、前記発明によって得られる運用保守装置においては、各サーバのディスク使用量などの情報を監視できることが示されているものの、その情報をどのように扱うかについての詳細が記述されておらず、上述したような運用保守が後手にまわってしまうという問題も解決できていない。

【0012】次に、分散システムの運用保守に関する他の技術としては、例えば、特開平7-21059号公報に示された発明がある。この発明は、分散システム内で発生する障害などについての情報を、一括して採取・収集・編集・転送できるような集中管理方式を導入することで、分散システムの構成要素単位ではなく、分散システム全体にわたる運用保守を可能にすることを目的としている。

【0013】また、前記集中管理方式の導入にあたっては、上述した特開平6-149737号公報に示された発明とは異なり、最上位の統合サーバ、営業部門の営業店サーバ、そしてクライアントからなる階層を構成し、運用保守に必要な情報が下位の階層から上位の階層に転送されていくようにすることで、集中管理を可能としている。さらに、この発明においては、運用保守に必要な情報の形式および内容を、オブジェクト指向の考え方に基づいて規定することを提案している。これによ

り、運用保守上必要な情報を、特定のソフトウェアなどの環境に依存しない形で管理することができるようにしている。

【0014】しかし、分散システムの運用保守にあたって、前記発明によっても解決されない課題がいくつか存在する。すなわち、業務毎に異なる特性が意識されないことに起因して、重点をおくべき運用保守対象が優先されて処理されず、また、すべての運用保守対象を同一レベルで扱うため、無駄なコストが発生するという点である。すなわち、この発明においても、業務アプリケーションの「意味」と分散システムとを関連付ける技術についてはなんら示されておらず、結果として、優先的に運用保守を行うべき対象を特定することができないまま、無駄な運用保守コストが発生している。

【0015】さらに、この発明においても、運用保守上必要な情報が管理者に伝わるのか、障害などが発生した後になってしまうので、運用保守が常に後手にまわってしまうという問題を生じていた。なお、この発明においては、「予防保守」という表現によって、運用保守が後手にまわってしまう課題を意識していることが表わされているが、定期的かつ定期的に分散システムの構成要素を管理すること以上の、具体的な運用保守の方法については言及されておらず、運用保守が後手にまわってしまう課題を解決できていないとはいえない。

【0016】また、分散システムの運用保守の観点に基づく他の技術としては、米国Hewlett-Packard社製の、HP OpenViewという製品がある（経産省データプロ・ソフト 1995年 2月号 p. 251-269）。この製品は大きくネットワーク管理製品群とシステム管理製品群に分かれている。ネットワーク管理製品群の中核となるのは、HP OpenView ネットワーク・ノード・マネージャと呼ばれる製品であり、SNMP（Simple Network Management Protocol）ベースで、ネットワークについての障害管理、構成管理、性能管理を行う。また、システム管理製品群の中核となるのは、HP OpenView Operations Centerと呼ばれる製品であり、SNMPベースで、システムについてのイベント管理、ソフトウェア配布、ファイル等のバックアップ、負荷状況の把握などを行う。

【0017】しかし、この製品によっても先に示した運用保守上の課題は解決されない。すなわち、この製品においても、分散システム上に実装されている業務アプリケーションの「意味」と分散システムとを関係的に関連付ける手段は提供されておらず、重点をおくべき運用保守対象が優先されて処理されず、また、すべての運用保守対象を同一レベルで扱うため、無駄なコストが発生するという問題が生じている。

【0018】確かに、ネットワーク管理のソフトウェアである HP OpenView History Ana-

lyzer では、特定のサービスを多く利用しているユーザの状況を把握でき、このことによって一瞬の局面では、業務の「意味」と分散システムの関連付けはなされているということができ、業務の持つ重要性は、ユーザのサービス利用数とは直接相関関係にあるとはいえない。例えば、非常に重要な事務業務などは、ごく限られたユーザがごく限られたタイミングでしかサービスを受けないものと考えられるからである。

【0019】さらに、この製品においては、システム管理のソフトウェアである HP Performance および HP PCs と呼ばれる製品によって、分散システムの構成要素に対しての性能管理データの収集および将来動向予測などのデータ分析を可能にしている。しかし、業務の特性を意識した、重点をおくべき運用保守対象を特定できていないため、データ分析を適切に行えず、結果として適切でない分析結果による運用保守が行われてしまう危険性があった。

【0020】

【発明が解決しようとする課題】上述したように、従来の分散システムの運用保守支援技術は、どの業務が重要であるかといった業務の持つ「意味」と、分散システムの構成要素を適切に関連付けるための十分な手段を提供しておらず、また、分散システムに対する適切な分析手段を提供しないまま、運用保守を支援していた。

【0021】その結果、解決すべき課題として次の3点が挙げられる。すなわち、（1）分散システムのエンドユーザがもっとも重要であると考えている業務に関連した運用保守対象が、優先して運用保守されない。（2）重要でない業務に関連した運用保守対象も、すべて平等に運用保守されてしまい、運用保守コストに無駄が発生してしまう。（3）運用保守対象を特定するための分析が適切に行えず、有効な運用保守計画を立案することができない。

【0022】本発明は、上述したような従来技術の課題点を解決するために提案されたもので、その目的は、分散システムの運用保守を効果的、経済的かつ的確に行えるようにした分散システム運用保守支援装置および運用保守方法を提供することにある。

【0023】

【課題を解決するための手段】上記の目的を達成するために、請求項1に記載の発明は、複数の計算機およびその周辺機器をネットワークを介して接続した分散システムに対する運用保守支援装置であって、前記分散システムの運用保守支援を開始し、さらにその後、運用保守支援動作を制御する運用保守制御手段と、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の指標として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、前記分

散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とするものである。

【0024】また、請求項5に記載の発明は、請求項1に記載の発明を方法の観点から捉えたものであり、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、前記分散システムの運用保守支援を開始し、さらにその後続く運用保守支援動作を制御する運用保守制御ステップと、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とするものである。

【0025】このような構成を有する請求項1に記載の分散システム運用保守支援装置あるいは請求項5に記載の分散システム運用保守支援方法においては、運用保守支援を進める上での全体的な流れを、運用保守制御手段が制御する。この流れは、運用保守制御手段内に保持されている起動を引く仕組みによって開始され、それとともに分散システムのエンドユーザがもっとも重要であると考えている業務が何であるかについての情報とそれに付随する情報が取得される。この段階で、エンドユーザにとって優先されるべき運用保守が正しく実働されることを保証され、効果的な運用保守が可能となる。さらに、業務仕様管理手段によって、分散システムのエンドユーザがもっとも重要であると考えている業務と、運用保守が必要になるかも知れない分散システム内の構成要素が関連づけられる。この段階で、無駄な運用保守コストの発生を抑えることができるようになり、経済的な運用保守が可能となる。

【0026】請求項2に記載の発明は、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援装置であって、前記分散システムの運用保守支援を開始し、さらにその後続く運用保守支援動作を制御する運用保守制御手段と、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、前記分散システムの構成要素の内、運用保守制御手段により指示された構成要素の将来的な動向を予測する予測手段と、前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とするものである。

【0027】また、請求項6に記載の発明は、請求項2

に記載の発明を方法の観点から捉えたものであり、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、前記分散システムの運用保守支援を開始し、さらにその後続く運用保守支援動作を制御する運用保守制御ステップと、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、前記分散システムの構成要素の内、運用保守制御ステップにおいて指示された構成要素の将来的な動向を予測する予測ステップと、前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とするものである。

【0028】このような構成を有する請求項2に記載の分散システム運用保守支援装置あるいは請求項6に記載の分散システム運用保守支援方法においては、請求項1あるいは請求項5に記載の発明と同様に、運用保守制御手段によって全体的な流れが制御され、業務仕様管理手段によって業務と分散システム内の構成要素が関連づけられる。次に、予測手段において、運用保守が必要になるかも知れない分散システム内の構成要素の将来動向を予測し、運用保守が必要であることが判明した分散システム内の構成要素のみを特定する。この段階で、請求項1あるいは請求項5に記載された発明よりも、さらに無駄な運用保守コストの発生を抑えることができるようになり、より経済的な運用保守が可能となる。また、それと同時に、予測結果をもとにした適切な分析によって、有効な運用保守計画を立案することができるようになり、計画的な運用保守が可能となる。

【0029】請求項3に記載の発明は、請求項2に記載の分散システム運用保守支援装置において、前記予測手段が、前記監視手段によって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とするものである。

【0030】また、請求項7に記載の発明は、請求項3に記載の発明を方法の観点から捉えたものであり、請求項6に記載の分散システム運用保守支援方法において、前記予測ステップが、前記監視ステップによって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とするものである。

【0031】このような構成を有する請求項3に記載の分散システム運用保守支援装置あるいは請求項7に記載の分散システム運用保守支援方法においては、適切な予測モデルから得られた予測結果をもとにして、適切な予

所を行うことができるので、有効な運用保守計画を立案することができるようになり、詳細な運用保守が可能となる。

【0032】請求項4に記載の発明は、請求項1乃至請求項3のいずれかに記載の分散システム運用保守支援装置において、前記運用保守制御手段が、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とするものである。

【0033】また、請求項8に記載の発明は、請求項4に記載の発明を方法の観点から捉えたものであり、請求項5乃至請求項7のいずれかに記載の分散システム運用保守支援方法において、前記運用保守制御ステップが、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とするものである。

【0034】このような構成を有する請求項4に記載の分散システム運用保守支援装置あるいは請求項8に記載の分散システム運用保守支援方法においては、管理者が当初はあまり重要でないと考えていた業務を見逃す危険性を低く抑えることができるようになるので、より確実な運用保守を実施することが可能となる。

【0035】

【発明の実施の形態】以下、本発明の実施形態について、図面を参照して具体的に説明する。

【0036】[1. 本発明による運用保守支援の全体像] 図1は、本発明による運用保守支援の全体像を示したものである。すなわち、運用保守の対象となる分散システム(以下、運用保守対象分散システムと称する)10は、エンドユーザ12によって各種業務に利用され、また、本発明に係る運用保守支援装置11によってその稼働が監視され、さらに、管理者13によって運用保守される。一方、運用保守支援装置11は、前記運用保守対象分散システム10の稼働を監視し、管理者13に対して運用保守支援を行う。また、エンドユーザ12は、運用保守対象分散システム10を業務に利用する上で、管理者13に対して、どの業務が重要かといった業務の「意味」を要求として伝え、また、管理者13から、運用保守対象分散システム10をどのようにして運用保守するかについてアナウンスを受ける。さらに、管理者13は、運用保守対象分散システム10を運用保守支援装置11の支援を受けながら運用保守し、また、エンドユーザ12に運用保守対象分散システム10をどのようにして運用保守するかについてアナウンスし、エンドユーザ12からどの業務が重要かといった業務の「意味」を要求として受けとる。

【0037】なお、前記運用保守対象分散システム10と運用保守支援装置11は、物理的に同じシステム11に実装されても、分けて実装されても良い。さらに、一層進化する形で実装されても良い。論理上、運用保守対象分散システム10と運用保守支援装置11の間の関

別がつけば良い。また、同様に、エンドユーザ12と管理者13が、実際には同一の個人、あるいは複数からなるグループでも構わない。

【0038】[2. 運用保守対象分散システムの構成] 図2は、運用保守対象分散システム10の詳細を示したものである。すなわち、運用保守対象分散システム10は、複数の計算機100(CPU103あるいはメモリ104などを含む)、およびその周辺機器であるディスク105、ネットワーク106などから構成されている。ここで、前記計算機100については、分散システムのアーキテクチャあるいはモデルによって、サーバ101やクライアント102といった区別を持たせることができる。なお周辺機器については、運用保守の必要性に応じてどのようなものを対象にするかが決まり、図2に示したディスク105に限定されるものではない。

【0039】また、この運用保守対象分散システム10には、本発明に係る運用保守支援装置11と連携するための、分散システム内監視手段107が含まれている。この分散システム内監視手段107は、CPU103やメモリ104、ディスク105、ネットワーク106などから、運用保守対象分散システムに必要な運用保守情報を収集する。すなわち、分散システム内監視手段107は、単にデータを収集する手段であり、既存の技術によって容易に構築できる部位である。例えば、従来の技術の項において挙げた HP OpenView では、HP OpenView Traffic Explorer/UNIX という製品によって、I/Oを測れるトラフィックを監視することかできる。なお、分散システム内監視手段107が行う収集の方法などについては、本発明に係る運用保守支援装置11から指示を受けて決定されるように構成されている。

【0040】[3. 運用保守支援装置の構成] 図3は、本発明の対象である運用保守支援装置11の構成を示したものである。すなわち、運用保守支援装置11は、以下に詳述する運用保守制御手段110、業務仕様管理手段111、予測手段112、監視手段113とから構成されている。

【0041】ここで、前記運用保守制御手段110は、管理者13から明示的な運用保守支援依頼を受けるか、内部的な動機が発生することによって、運用保守支援を開始し、さらにその後続く運用保守支援の一連の動作を制御するものである。また、前記業務仕様管理手段111は、業務を体現するアプリケーションと、それが実装される分散システムとの間の対応関係を仕様として管理しており、前記運用保守制御手段110からの問い合わせに応じて、必要な情報を提供するものである。さらに、前記予測手段112は、前記運用保守制御手段110から指示された、運用保守が必要と思われる分散システムの構成要素に対して、将来的な動向を予測するものである。また、監視手段113は、運用保守対象分散シ

システム10内に含まれている前記分散システム内監視手段107に、データウェアハウスとしての側面を与え、すなわち、運用保守上必要なデータの収集の仕方に際して指示を与え、前記予測手段112が必要とする運用保守情報を収集させ、収集された運用保守情報を予測手段112に伝えるものである。

【0042】なお、運用保守対象分散システム10内の監視手段107は、単なるデータ収集の手段であったが、これに対して、運用保守支援装置11内の監視手段113は、分散システム内監視手段107から取り出したデータを用いて、運用保守上利用しやすいような形式に変換するといった付加的な機能を有している。

【0043】1-2-1. 運用保守制御手段の構成 図4は、前記運用保守制御手段110の構成を示したものである。すなわち、運用保守制御手段110は、以下に詳述する窓口1110あるいはタイマ1101、またはその両方と、運用保守制御リスト1102、予測対象リスト1103、要求特性データ1104、予測データ1105、判断部1106および運用保守対象リスト1107とから構成されている。

【0044】(窓口) 窓口1110は、管理者13が明示的、黙示的に、運用保守対象分散システム10の運用保守支援を受けようとしたときの窓口となる。すなわち、管理者13が、窓口1110から、どの業務について運用保守を行うかを入力することによって、運用保守制御手段110による制御が開始される。

【0045】ここで、図5は、窓口1110で行われる前記入力処理を受け付ける画面の一例を示したものである。すなわち、図5に示した例においては、「業務」と、その業務が投入される「ノード」が入力できるようになっている。また、ボタン20は、運用保守の必要があるかどうかが簡単にチェックされる業務をまとめて指定できるボタンである。一方、運用保守の必要があるかどうかを個別にチェックしたい場合には、リストボックス21から所望の「業務」を個別に選んで指定することもできる。さらに、ボタン22は、ボタン20あるいはリストボックス21で選ばれた業務が通常投入されるノードをまとめて指定できるボタンである。一方、業務投入ノードを個別に指定したい場合には、リストボックス23から指定することもできる。なお、窓口1110から入力される情報、および窓口1110が提供するガイダンスは、必ずしも上記の通りでなくとも良い。

【0046】(タイマ) タイマ1101は、管理者13が明示的、黙示的に運用保守を行おうとしない場合でも、運用保守支援装置11として自動的に運用保守支援を行うために必要とされるものである。すなわち、予めタイマ1101に設定された日時・時刻になると、運用保守制御手段110による制御が開始されるように構成されている。

【0047】(運用保守制御リスト) 前記窓口1110

あるいはタイマ1101によって、運用保守制御手段110が起動されると、運用保守制御リスト1102に記述された内容にしたがって、どの業務を運用保守の対象とするかが決定される。

【0048】ここで、図6は、運用保守制御リスト1102の一例を示したものである。すなわち、窓口1110においてデフォルト業務が指定されたときには、受注業務と発注業務を対象とし、さらに窓口1110においてデフォルトノードが指定されたときには、東京都と大阪を対象とすることが記述されている。また、図6の例では、タイマ1101によって起動される場合、毎月1日の午前4時と毎日午前7時に運用保守制御手段110を起動し、それぞれの場合に対象とすべき業務が何であるかが記述されている。なお、運用保守制御リスト1102に記述する内容および記述の方法は、必ずしも上記の通りでなくとも良い。

【0049】(予測対象リストおよび要求特性データ) 運用保守制御手段110は、前記運用保守制御リスト1102の内容をもとに、業務係数管理手段111に関わり、合わせを行い、業務に関連して運用保守の対象となり得る分散システムの構成要素(CPU1103やメモリ1104、ディスク1105、ネットワーク1106など)を記述した予測対象リスト1103、およびそれらの構成要素が満たすべき特性を要求として記述した要求特性データ1104を得る。

【0050】ここで、図7は、予測対象リスト1103の一例を示したものである。すなわち、図7の例では、予測を行うべき運用保守対象分散システム10内の構成要素として、「server」と名付けられているサーバのCPU、メモリ、ディスク、および「client」と名付けられているクライアントのCPU、メモリ、ディスク、および「server」と「client」とを結ぶネットワーク、および「server」と「client」とを結ぶネットワークが指示されている。なお、予測対象リスト1103に記述する内容および記述の方法は、必ずしも上記の通りでなくとも良い。

【0051】また、図8は、要求特性データ1104の一例を示したものである。すなわち、図8の例では、予測を行うべき運用保守対象分散システム10内の構成要素が満たしていなければならない特性として、「server」と名付けられているサーバについて、そのCPUの最大負荷/平均負荷がどのようでなければならないか、およびメモリの最大ページフォールト数/平均ページフォールト数がどのようでなければならないか、およびディスクの読取り/書き込みがどのようでなければならないかといった情報が示されている。また、同様の内容が、「client」と名付けられているクライアントについても示されている。さらに、「server」と「client」とを結ぶネットワーク、および「server」と「client」とを結ぶネットワークについて、それらの間を

13

演れる最大バケット数/平均バケット数かどのようである
なければならないかが示されている。なお、この要求特性
データ1104に載せられるデータは、後述する業務仕
様管理手段111から得られるように構成されている。
また、要求特性データ1104に記述する内容および記
述の方法は、必ずしも上記の通りでなくとも良い。

【0052】(予測データ)さらに、運用保守制御手段
110は、予測対象リスト1103の内容を前記予測手
段112に引き渡し、それぞれの分散システムの構成要
素の予測趣向を、予測データ1105として得る。この
予測データ1105は、ある時系列なデータとして得ら
れる。

【0053】図8は、予測データ1105の一例を示し
たものである。すなわち、予測が行われた運用保守分散
システム10内の構成要素の予測趣向として、1日単位
で各構成要素がどのように推移するかを示している。
なお、予測データ1105に記述する内容、記述の方法
および予測の時間間隔/期限などは、必ずしも上記の通
りでなくとも良い。

【0054】(判断部)さらに、運用保守制御手段11
0は、判断部1106において、運用保守制御リスト1
102と要求特性データ1104と予測データ1105
の内容を比較することにより、管理者13に通知すべき
運用保守対象リスト1107を作成する。

【0055】ここで、前記判断部1106の動作につ
いて説明する。まず、要求特性データ1104からデータ
を一つ取り出す(ステップ1001)。例えば、図8に
示した要求特性データ1104の例では、“svr1”
のCPUについての平均負荷が0.1以下でなければ
ならない”といったデータを取り出す。次に、予測デ
ータ1105のうち、現在に最も近い予測時点を選
び(ステップ1002)、予測データ1105から該当す
るデータを取り出す(ステップ1003)。例えば、図
9に示した予測データ1105の例では、現在に最も近
い予測時点である昨日(=1day)を選ぶ。そして、
その時点での予測値が、前記要求特性データ1104に
示された要求値を超えているか否かを判定し(ステッ
プ1004)、越えている場合には、その構成要素を「問
題あり」として記録する(ステップ1005)。例え
ば、図9に示した予測データ1105の昨日(=1da
y)の例では、“svr1”のCPUについての平均負
荷は“0.12”であり、図8に示された要求特性デ
ータ1104の要求値である“0.1”を超えているの
で、その時点を記録する。そして、要求を超えていたこと
がわかった場合には、その時点をもってその構成要素の問
題発生時点とし、それ以降については、その構成要素に
ついては調べない。

【0056】一方、要求を超えていなければ次の予測時
点に移り(ステップ1006)、その予測時点における

14

予測値が、前記要求特性データ1104に示された要求
値を超えているか否かを判定し(ステップ1004)。
越えている場合には、その構成要素を「問題あり」とし
て記録する(ステップ1005)。そして、同様の処理を
予測データが尽きるまで繰り返す(ステップ1007)。
例えば、図9に示した予測データ1105の場合
には、問題が発生されない限り、10日後(=10da
y)まで調べ続けられる。上記の処理を、要求特
性データ1104に示されたすべてのデータについて繰
り返す(ステップ1008、ステップ1009)。

【0057】要求特性データ1104に示されたすべての
のデータについて、上記の処理が終了した後、判断部
1106においては、運用保守制御リスト1102から重
要業務をつ取り出す(ステップ1010)。例えば、
図9に示した運用保守制御リスト1102の例では、重
要業務として「受注業務」が選ばれている。さらに、事前の
処理(ステップ1001～ステップ1009)による記
録から、問題が発生する構成要素をつ取り出す(ステ
ップ1011)。例えば、先の例では、“svr1”
のCPUが選ばれている。

【0058】このとき、後述する業務仕様管理手段11
1に関わり合わせて、重要業務かその構成要素を含んで
いるか否かを判断する(ステップ1012)。そして、重
要業務かその構成要素を含んでいる場合には、その構成
要素に問題が発生する時点が、その重要業務を構成する
他の構成要素に問題が発生する時点より早い(か否かを)
調べ(ステップ1013)。それらのどちらよりも早い発生
時点であれば、その構成要素を問題発生時点とし、か
つ、その発生時点を重要業務の問題発生時点とし(ステ
ップ1014)。「どの重要業務に、いつ、何の問題が
発生するか」を、運用保守対象リスト1107に載せる
(ステップ1015)。例えば、先の例では、重要業
務として選ばれた「受注業務」が、“svr1”のCPU
の平均負荷の増大により、昨日に問題を引き起
こす”といった内容が、運用保守対象リスト1107に
記述される。

【0059】また、原因に対する対策を示すことかでき
る場合には、合わせてその対策も運用保守対象リス
ト1107に示される(ステップ1016、ステップ101
7)。このような対策を示すためには、様々な方法が考
えられるが、一つの方法としては、個々の構成要素毎
に、それか原因となった場合の対策についての情報を持
たせ、これを業務仕様管理手段111において直接管理
させる方法が考えられる。また、判断部1106内に判
断知識をルール化したものを置き、それを参照させる方
法なども考えられる。

【0060】以上の対応付けを、事前の処理(ステッ
プ1001～ステップ1009)による記録のすべてにつ
いて繰り返す(ステップ1018、ステップ101
9)。さらに、運用保守制御リスト1102に基づいて

50

たすべての重要業務について、上記処理を繰り返す（ステップ1020、ステップ1021）。

【0061】（運用保守対象リスト）次に、前記運用保守対象リスト1107について説明する。すなわち、図13は、運用保守対象リスト1107の一例を示したものであるが、この例では、将来的に支障が出る業務とその日時および原因、さらに運用保守が必要な分散システム110内の構成要素が格納されており、これが管理者13に通告されることになる。

【0062】管理者13は、この運用保守対象リスト1107を参照することによって、運用保守対象分散システム110に問題が発生する前にそれを検知し、運用保守が必要な構成要素についてだけ、計画的に運用保守を実施することができるようになる。さらに、エンドユーザ12は、運用保守対象リスト1107にしたがってなされる管理者13からのアナウンスによって、突然十分なサービスを受けられなくなる状況を回避できるようになる。

【0063】「3-2. 運用保守制御手段における制御の流れ」図14は、運用保守制御手段110における制御の流れを示したものである。すなわち、管理者13が、図11100から、どの業務について運用保守を行うかを入力することによって、運用保守制御手段110による制御が開始される（ステップ141）。あるいは、所定の日時/時刻を設定したタイマ1101によって、運用保守制御手段110による制御が自動的に開始される（ステップ142）。

【0064】続いて、運用保守制御手段1102に記述された内容にしたがって、どの業務を運用保守の対象とするかが決定され（ステップ143）、また、運用保守制御手段1102の内容をもとに、業務仕様管理手段111に問い合わせることにより、運用保守の対象となり得る分散システムの構成要素を記述した予測対象リスト1103、およびそれらの構成要素が満たすべき特性を要求として記述した要求特性データ1104が得られる（ステップ144）。

【0065】次に、予測手段1112に予測を依頼することにより、それぞれの分散システムの構成要素の予測動向が、予測データ1105として得られる（ステップ145）。また、判断部1106において、運用保守制御手段1102と要求特性データ1104と予測データ1105の内容が比較される（ステップ146）。運用保守対象リスト1107が作成されて、管理者13に通告される（ステップ147）。

【0066】「3-3. 業務仕様管理手段の構成及び作用」図15は、業務仕様管理手段111の構成を示したものである。すなわち、業務仕様管理手段111は、その内部に「業務」とその業務に関連した運用保守対象分散システム110の構成要素との関係を保持したデータベース1110を保持している。また、このデータベース

1110では、業務1111、プロセス1112、テーブル1113、ノード1114、CPU1115、メモリ1116、ディスク1117、ネットワーク1118の各構成要素と、各構成要素間の関係が管理されている。なお、図15に示したデータベースにおいては、それぞれの関係をエンティティリレーションシップ図を用いて表している。また、ここでいう「ノード」とは、例えば、一つのIPアドレスを持つような計算機のことを意味している。

【0067】次に、前記データベース1110をリレーショナルデータベースとして構築したときに、業務1111やプロセス1112などかどのように格納されるかについて、図16～図23を参照して説明する。

【0068】すなわち、図16には、「業務」について記述したテーブル（A）と、業務に関連する「プロセス」を記述したテーブル（B）の2つが示されている。そして、この2つのテーブルから、「ある業務がどのようなプロセスから構築されているか」、また「その業務がどれだけの時間で処理を終えなければならないか」についての情報を得ることができる。

【0069】また、図17には、「プロセス」について記述したテーブル（A）と、プロセスが構築されている「ノード」を記述したテーブル（B）と、プロセスが処理の対象とする「テーブル」およびその配置先を記述したテーブル（C）の3つが示されている。そして、この3つのテーブルから、「どのプロセスかどのノードで実行される」、「どのノードにあるどのテーブルにアクセスするか」、また「実行にあたって、どれだけの処理時間とメモリを消費するか」についての情報を得ることができ、なお、処理時間としては、仮定されたある処理性能を有する標準的な計算機によって処理が実行された場合に、必要とされる時間が表示されている。

【0070】次に、図18には、「テーブル」について記述したテーブル（A）と、テーブルが配置されている「ノード」を記述したテーブル（B）の2つが示されている。また、図19には、「ノード」について記述したテーブル（A）と、ノードが保持しているCPU、メモリ、ディスク、ネットワークとの関連を記述したテーブル（B）～（E）の5つが示されている。さらに、図20には「CPU」について記述したテーブルが記述され、図21には「メモリ」について記述したテーブルが記述されている。また、図22には、「ディスク」について記述したテーブルが記述され、図23には、「ネットワーク」について記述したテーブルが記述されている。

【0071】そして、上記の図20から図23までに示された各テーブルの値は、図16で示された業務1111のレスポンスタイムを満たすことができるように決定されている。例えば、受注業務（業務1100）のレスポンスタイムは3秒であることが要求されており

(図16参照)。このとき受注業務によって使用される受注プロセス(プロセス111=101)の処理時間が300であり(図17参照)。さらに、“svr1”のCPUについてみると、その性能は標準として設定されたCPUの2倍の性能であることから(図20参照)、“svr1”のCPUがそれぞれ最大負荷が2、平均負荷が0.1を越えては受注業務に要求されているレスポンスタイムを実現できない」といった判断を管理者13が行うことで、値が決定される。

【0072】なお、業務仕様管理手段111あるいはデータベース1110が管理する、上記図16から図23までに示されている構成要素の種類、管理方法については、必ずしも上記の通りでなくとも良い。

【0073】3-4. 予測手段の構成及び作用 図24は、予測手段112の構成を示したものである。すなわち、予測手段112は、その内部に、運用保守制御手段110から引き継いだ予測対象リスト1103と、各構成要素毎に適用される予測モデル1121、各構成要素毎の過去の推移リスト1120、各構成要素毎の予測データ112と、および運用保守制御手段110に引き継ぎ予測データ1105を保持している。

【0074】ここで、各構成要素毎に適用される予測モデル1121は、予測を行いたい構成要素の過去の推移リスト1120と、他の構成要素の過去の推移リスト1120とを組み合わせて使用される。例えば、CPUの負荷予測を行うことを考えた場合、当然のことながらCPU自身の過去の推移も参照するべきであるし、また、メモリの影響を受けるのであれば、メモリについての過

*去の推移を参照しても良い。さらに予測モデル1121は、統計的な算術式によるものでも良いし、いわゆるニューラルネットワークモデルに基づくような自己学習型の予測手段をモデル化したものでも良い。

【0075】そして、最終的に予測手段112は、各構成要素毎の予測データ1122を編集してまとめ、予測データ1105として運用保守制御手段110に引き継ぎように構成されている。

【0076】(統計的な手段を用いた予測モデルの一例) ここで、統計的な手段を用いた予測モデルの一例として、ディスク105の使用量の将来動向の予測を扱う。なお、予測にあたっては、次の2つの前提を置く。すなわち、(1) ディスク105の使用量は、ユーザ数と強い相関関係にある。(2) ユーザ数は、時間と共に直線的に増加する。

【0077】このような前提のもとでは、先にユーザ数の変化を予測し、それを基にディスク105の使用量の変化を予測することになる。まず、ある時刻x、のもとでユーザ数がy;であったとすると、前提(2)より、両者の関係は次のように表わされる。

【0078】
【数1】 $y = ax + b$ … (1)
上式における“a”および“b”は、増加(あるいは減少)傾向を示すための係数である。この“a”および“b”を最小2乗法によって求めるために、以下の連立方程式を解く。

【0079】
【数2】

$$\begin{cases} a \sum_{i=1}^n x_i^2 + b \sum_{i=1}^n x_i = \sum_{i=1}^n x_i y_i \\ a \sum_{i=1}^n x_i + nb = \sum_{i=1}^n y_i \end{cases} \quad \text{----- (2)}$$

すると、解は、以下になる。

【0080】

$$\begin{cases} a = \frac{\frac{\sum_{i=1}^n x_i y_i - \frac{1}{n} \sum_{i=1}^n x_i \sum_{i=1}^n y_i}{\sum_{i=1}^n x_i^2 - \left(\frac{1}{n} \sum_{i=1}^n x_i \right)^2}}{\frac{\sum_{i=1}^n x_i - \frac{1}{n} \sum_{i=1}^n x_i \sum_{i=1}^n y_i}{\sum_{i=1}^n x_i^2 - \left(\frac{1}{n} \sum_{i=1}^n x_i \right)^2}} \\ b = \frac{\frac{\sum_{i=1}^n x_i \sum_{i=1}^n y_i - \frac{1}{n} \sum_{i=1}^n x_i^2 \sum_{i=1}^n y_i}{\sum_{i=1}^n x_i^2 - \left(\frac{1}{n} \sum_{i=1}^n x_i \right)^2}}{\frac{\sum_{i=1}^n x_i - \frac{1}{n} \sum_{i=1}^n x_i \sum_{i=1}^n y_i}{\sum_{i=1}^n x_i^2 - \left(\frac{1}{n} \sum_{i=1}^n x_i \right)^2}} \end{cases} \quad \text{----- (3)}$$

次に、以上によって求められたユーザ数y;を基に、ディスク105の使用量xiを求める。前提(1)より、両者の関係は以下のような回帰直線によって表わされる。なお、この回帰直線は、xのyへの回帰直線とする。

※【数3】

【0081】
【数4】
$$x = \frac{\sigma_y}{\sigma_x} \rho_{xy} y + \bar{x} - \frac{\sigma_x}{\sigma_y} \rho_{xy} \bar{y} \quad \text{----- (4)}$$

上式において、 σ_y はyの標準偏差、 σ_x はxの標準偏

差、 ρ_{xy} は y と x の相関係数を表し、 y の平均値は \bar{y} の上にバーを付し、 x の平均値は \bar{x} の上にバーを付して表している。

【0082】以上に示した一連の式(1)から式(4)が予測モデルとして機能することによって、ディスク105の使用量の将来動向を予測することが可能となる。

【0083】(自己学習的な手段を用いた予測モデルの一例)次に、自己学習的な手段を用いた予測モデルの一例として、ネットワーク106の負荷の将来動向の予測を扱ってみる。なお、ここでは自己学習型の予測手段として、図25に示すような多層型ニューラルネットワーク30を採用するものとする。また、予測にあたって、ネットワーク106の負荷は、自己の過去の推移から予測可能であるという前提を置く。さらに、このニューラルネットワーク30を構成するニューロン32は、図26に示すようなシグモイド関数31と呼ばれる非線形モデルによって表現されるものとする。

【0084】まず、本予測手段112を含んだ運用保守支援装置11の利用に先立って準備を行う。すなわち、ネットワーク106の負荷の過去の推移を教師値として、対応する入力値33の値34(=x)およびネットワークの重みに基づく出力値37の値38(=x)との誤差が最小になるように、ニューロン間の重み係数39(=w)を更新しておく。

【0085】なお、この学習のためには、バックプロパゲーション法が用いられる。また、予測を行うには、予測を行おうとする時点および、それより過去の時点のネットワーク106の負荷からなる値のリストx=

(x1, x2, x3, . . . , xn)を人力として、以下の式(5)から式(8)によってネットワークの出力値38(=x)が求められる。

【0086】

【数5】

$$g_j(x) = \sum_{i=1}^n (w_{ij} x_i) \quad \text{----- (5)}$$

【数6】

$$y_j(x) = \frac{1}{1 + \exp(-g_j(x))} \quad \text{----- (6)}$$

【数7】

$$g(x) = \sum_{j=1}^m (w_{jy} y_j(x)) \quad \text{----- (7)}$$

【数8】

$$x(x) = \frac{1}{1 + \exp(-g(x))} \quad \text{----- (8)}$$

なお、入力値34や中間値36、あるいは出力値38は、実際の値から正規化/逆正規化して扱う必要があ

る。すなわち、ネットワーク106の負荷の場合、実際に流れるパケットの量を表す数値や数値といった値を正規化して0近傍の値に変換してから入力値34とした。り、0から1の間までの値として出力された出力値も逆正規化して実際のパケット量を表すようにしてやる必要がある。この正規化/逆正規化は、ニューラルネットワークの反応性を高めるという意味からも必要ものである。

【0087】以上に示した多層型ニューラルネットワークが予測モデルとして機能することによって、ネットワーク106の負荷の将来動向を予測することが可能となる。また、このような自己学習型の予測モデルを採用することで、どの時間帯に業務が集中するかといった情報を明示的に示さなくても、それらの情報を考慮できるようにする。

【0088】(4. 本実施形態の運用保守支援装置の効果)上述したように、本実施形態の運用保守支援装置においては、この装置を構成する上記各手段によって、「どの業務を運用保守の対象とすべきか」、「その業務に関連する分散システム内の構成要素は何か」、「その構成要素が満たすべき特性はどのようなものか」、「その構成要素の将来的な動向はどのようなものか」といった観点で、分散システムの運用保守を支援する処理が進められる。

【0089】その結果、重要な業務に関連した運用保守対象を優先して運用保守することができ、また、運用保守に対して優先度をつけることができるので、無駄な運用保守コストの発生を抑えることができる。さらに、運用保守を行うための分析が適切に行えるので、有効な運用保守計画を立てることができる。

【0090】

【実施例】以下に、より具体的な実施例を用いて、運用保守が想定される幾つかの場面において、本発明が提案する運用保守支援装置および方法によって得られる作用・効果について説明する。

【0091】まず始めの例として、World Wide Webを利用した情報提供を行うための分散システムを取り上げる。図27は、この分散システムの概要を示したものである。すなわち、図27において、分散システム50では、ネットワーク53に接続された多数のクライアント52が、HTTP(Hyper Text Transfer Protocol)サーバ51aおよび51bへアクセスする。また、この分散システム50のエンドユーザ54は、この分散システム50を利用して、情報検索を行うものとする。

【0092】ここで、情報検索には2種類あり、随時随到に行われ、結果も数秒で返ってこないといけない検索処理50aと、予め定めてそれより頻繁でもよく、結果も翌日返ってこればよい検索処理50bがあるものとする。なお、想定している状況では、クライアント52の

が教が、なおも日に日に増加している途中であるとする。

【0093】これまでの運用保守技術では、クライアント52の付数の増加に伴って、分散システム50内のすべての構成要素の増強を検討しなければならず、その結果、実施する運用保守も必ずしも適切なものであるという保証はなかった。

【0094】しかしながら、本発明による運用保守技術では、管理者55が運用保守支援装置から運用保守支援を受けることにより、業務の「意味」を考慮した適切な運用保守を行うことができるようになる。すなわち、上述した図1から図24にしたがって説明すると、管理者55が任意の時点で運用保守支援を受けるために窓11100を介するか、あるいはタイム1101に設定された11時になるかのいずれかによって、運用保守支援装置111が起動される。この運用保守支援装置111内の運用保守制御手段110は、窓11100あるいは運用保守制御リスト1102から得られる情報（業務や、それに対する付随情報）により、運用保守の対象となる業務を特定し、業務仕様管理手段111に運用保守の必要があるかも知れない分散システム50内の構成要素の選択を依頼する。

【0095】続いて、業務仕様管理手段111は、預定された業務と、業務仕様管理手段111内で管理されているデータベース1110内の情報と照らし合わせることで、分散システム50内において運用保守が必要になるかも知れない構成要素のみを選び出す。本例においては、重要な業務であると考えられる検索処理50aに関連した構成要素のみが選ばれ、検索処理50bだけに関連した構成要素は選ばれない。

【0096】この結果、運用保守制御手段110は、検索処理50aが行われる日TTPサーバ51aについて、記載された予測対象リスト1103と、「検索処理50aは、数秒で処理を終えなければならない」という要求特性データ1104を得る。さらに、運用保守制御手段110は、予測手段112に対して、日TTPサーバ51aに関して、それに接続されるクライアント52の増加に関連したCDROMメモリ、あるいはディスク、ネットワークなどの構成要素の将来動向を、それぞれの過去の稼働状況とモデルに照らし合わせて予測するよう依頼する。

【0097】この予測の結果は、予測データ1105として運用保守制御手段110に渡され、判断部1106が運用保守制御リスト1102および要求特性データ1104と照らし合わせることで、運用保守11問題が発生する箇所とその時期を判断し、運用保守対象リスト1107としてまとめ、最終的に管理者55に提示される。

【0098】〔5. 他の実施形態〕本発明は、上述した実施形態に限定されるものではなく、運用保守支援装置を運用保守制御手段110、業務仕様管理手段111及

び監視手段113のみから構成することも可能である。なお、この場合は、分散システムのエンドユーザがもっとも重要であると考えている業務に関連した運用保守対象が優先して運用保守され、かつ、重要な業務に関連した運用保守対象が重点的に運用保守されることで、無駄な運用保守コストの発生を抑えることができる。

【0099】また、前述運用保守制御手段110に設けられる窓11100において、運用保守すべき業務の重要度を自動的に設定できるように構成することもできる。すなわち、図28に示したように、窓11100には、保守指示が業務データベース11000と関連11001が備えられている。なお、この保守指示は業務データベース11000は、窓11100から管理者13が運用保守対象業務及び業務提示ノード等を指示するたびに、その業務が指示されたのは何回か、あるいはその業務に対してそのノードが指定されたのは何回かなどの情報を格納するものである。また、関係11001は、窓11100に予め設定されており、業務あるいは業務とノードの組み合わせについての保守指示回数がこの値を越えた場合には、運用保守制御リスト1102にその業務を重要業務として記載すべきか否かの判断が必要であるとの判断を下す基準となるものである。

【0100】そして、この判断の結果、その保守指示回数が関係11001を越えた業務を重要業務として自動的に運用保守制御リスト1102に追加しても良いし、図29に示したように、ダイアログボックスなどのユーザーインターフェースを提供することにより、管理者13の了解を得たあとで運用保守制御リスト1102に追加しても良い。

【0101】このように構成することにより、管理者13が当初はあまり重要でないと考えていた業務を見逃す危険性を低く抑えることができるようになる。なお、前述保守指示履歴データベース11000に格納する内容は、上述したものに限定されるものではなく、また、関係11001についても、すべての業務あるいは業務とノードの組み合わせについて同じ値に設定しても、異なる値に設定しても良い。

【0102】

【発明の効果】以上説明したように本発明によれば、分散システム上に実施される業務の「意味」を考慮することによって、分散システムのエンドユーザがもっとも重要であると考えている業務に関連した運用保守対象が優先して運用保守され、かつ、重要な業務に関連した運用保守対象が重点的に運用保守されることで、無駄な運用保守コストの発生を抑えることができる。かつ、運用保守を行うための分析が適切に行え、有効な運用保守計画を立てることができるようになる。

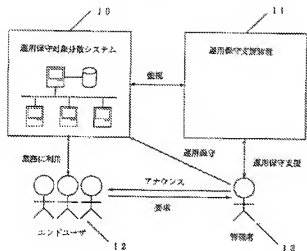
【図面の簡単な説明】

【図1】本発明による運用保守支援の全体像

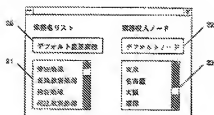
【図2】運用保守対象分散システムの構成図

- 【図3】運用保守支援装置の構成図
 【図4】運用保守制御手段の構成図
 【図5】「窓口」で行われる入力処理を受け付ける画面の一例を示す図
 【図6】運用保守制御リストの一例を示す図
 【図7】予測対象リストの一例を示す図
 【図8】要求特性データの一例を示す図
 【図9】予測データの一例を示す図
 【図10】判断部における制御の流れの前段階を示すフローチャート
 【図11】判断部における制御の流れの中段階を示すフローチャート
 【図12】判断部における制御の流れの後段階を示すフローチャート
 【図13】運用保守対象リストの一例を示す図
 【図14】運用保守制御手段の制御の流れを示すフローチャート
 【図15】業務仕様管理手段の構成図

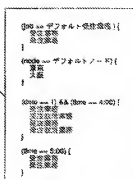
【図1】



【図5】

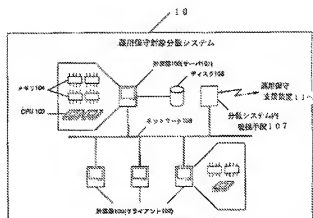


【図6】



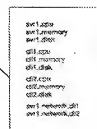
予測対象リスト102

【図2】

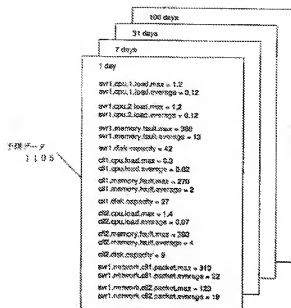


【図7】

予測対象リスト102



【図9】



【図13】

受注業務のレスポンスタイムが7日後に要求を満たさなくなる見込みです。

直接の原因は、本社サーバのCD-ROMの平均負荷がオーバーするためです。

本社サーバのメモリを増設することにより、解決されるものと思われます。

【図16】

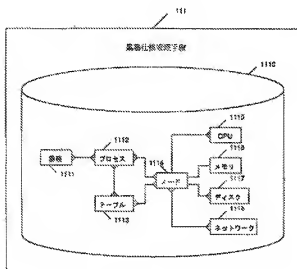
機器ID	要求値	レスポンスタイム
100	受注業務	2 sec
101	受注取寄せ	6 sec
102	受注業務	7 sec
103	受注業務	7 sec

機器ID	プロセスID
100	100
100	101
100	102
101	100
101	103
102	100
102	104
102	105
103	100
103	105

(A)

(B)

【図15】



【図17】

プロセスID	プロセス名	最大処理	メモリ量
100	受注入力	10	500
101	受注	200	1000
102	受注	5	50
103	受注取寄せ	600	1000
104	受注	400	1000
105	受注取寄せ	700	1000

(A)

(B)

プロセスID	ノードID
100	opt
101	opt
102	opt
103	opt
104	opt
105	opt

(C)

プロセスID	データベース	ノードID
101	100	opt
103	100	opt
104	101	opt
105	101	opt

【図18】

データベースID	データベース名	レコードサイズ
100	受注	1000
101	受注	1000

(A)

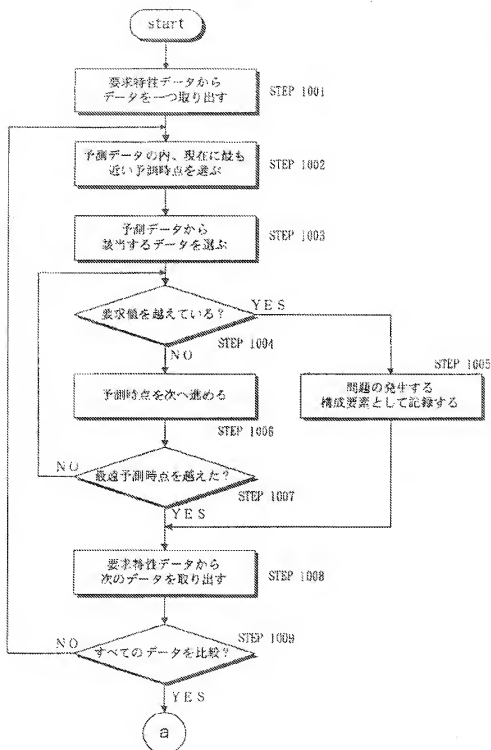
データベースID	ノードID
100	opt
101	opt

(B)

【図20】

CPU ID	処理時間	最大処理	受注業務
100	2	2	0.1
101	2	2	0.1
102	1	1	0.1
103	1	2	0.1

【図10】



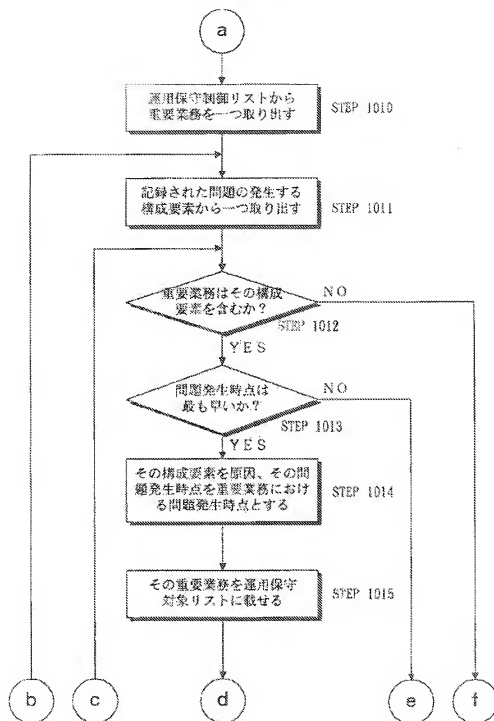
【図29】



【図23】

ネットワーク名	モード21	モード22	最速バケット数	平均バケット数
100	800	800	800	100
100	800	800	800	100

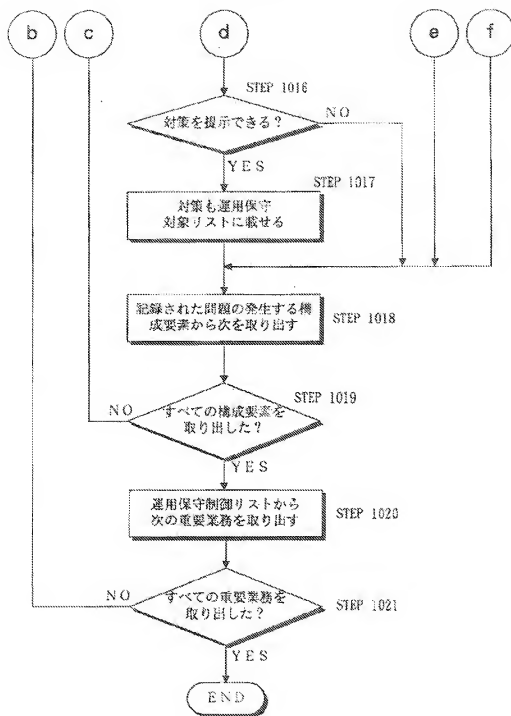
【図11】



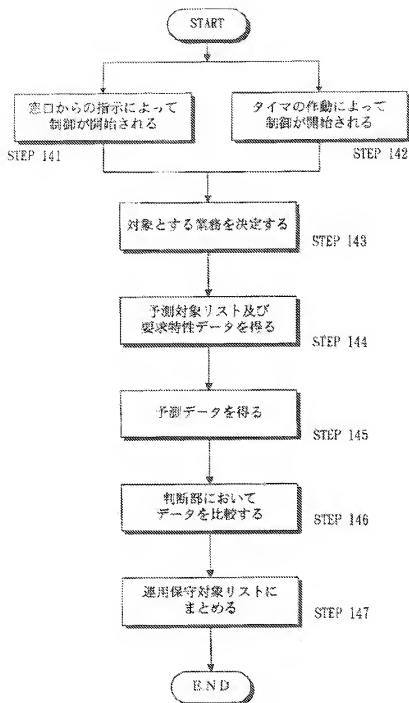
【図12】

メモリID	基本ページフォーマット数	変換ページフォーマット数
100	1000	10
101	1000	10
102	1000	10

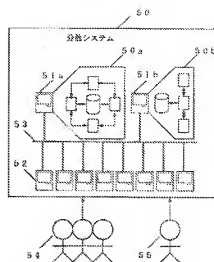
【図12】



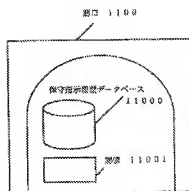
【図14】



【図27】



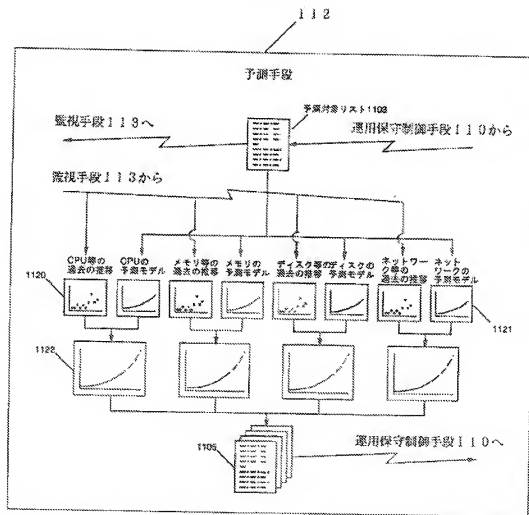
【図28】



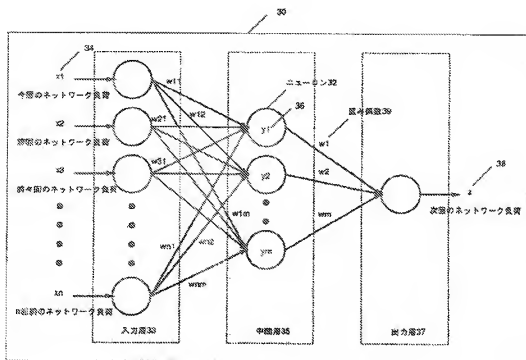
【図19】

(A)	<table border="1"> <thead> <tr> <th>ノードID</th><th>ノード名</th></tr> </thead> <tbody> <tr> <td>sw1</td><td>本局</td></tr> <tr> <td>st1</td><td>基局</td></tr> <tr> <td>st2</td><td>天線</td></tr> </tbody> </table>	ノードID	ノード名	sw1	本局	st1	基局	st2	天線		
ノードID	ノード名										
sw1	本局										
st1	基局										
st2	天線										
(B)	<table border="1"> <thead> <tr> <th>ノードID</th><th>CPUID</th></tr> </thead> <tbody> <tr> <td>sw1</td><td>100</td></tr> <tr> <td>st1</td><td>101</td></tr> <tr> <td>st2</td><td>102</td></tr> <tr> <td>st3</td><td>103</td></tr> </tbody> </table>	ノードID	CPUID	sw1	100	st1	101	st2	102	st3	103
ノードID	CPUID										
sw1	100										
st1	101										
st2	102										
st3	103										
(C)	<table border="1"> <thead> <tr> <th>ノードID</th><th>メモリID</th></tr> </thead> <tbody> <tr> <td>sw1</td><td>100</td></tr> <tr> <td>st1</td><td>101</td></tr> <tr> <td>st2</td><td>102</td></tr> </tbody> </table>	ノードID	メモリID	sw1	100	st1	101	st2	102		
ノードID	メモリID										
sw1	100										
st1	101										
st2	102										
(D)	<table border="1"> <thead> <tr> <th>ノードID</th><th>ディスクID</th></tr> </thead> <tbody> <tr> <td>sw1</td><td>100</td></tr> <tr> <td>st1</td><td>101</td></tr> <tr> <td>st2</td><td>102</td></tr> </tbody> </table>	ノードID	ディスクID	sw1	100	st1	101	st2	102		
ノードID	ディスクID										
sw1	100										
st1	101										
st2	102										
(E)	<table border="1"> <thead> <tr> <th>ノードID</th><th>ネットワークID</th></tr> </thead> <tbody> <tr> <td>sw1</td><td>100</td></tr> <tr> <td>st1</td><td>100</td></tr> <tr> <td>st2</td><td>100</td></tr> </tbody> </table>	ノードID	ネットワークID	sw1	100	st1	100	st2	100		
ノードID	ネットワークID										
sw1	100										
st1	100										
st2	100										

【図24】



【図25】



【図26】

